



BEC 6200WZL *Series*

4G/LTE Cellular Broadband Router

User Manual

Version release: v1.10

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION	6
INTRODUCTION TO YOUR ROUTER	6
FEATURES & SPECIFICATIONS	8
HARDWARE SPECIFICATIONS	10
APPLICATION DIAGRAM	10
CHAPTER 2: PRODUCT OVERVIEW	11
IMPORTANT NOTE FOR USING THIS ROUTER	11
DEVICE DESCRIPTION	12
Front Panel LEDs	12
Rear Panel Connectors	13
CABLING	14
CHAPTER 3: BASIC INSTALLATION	15
NETWORK CONFIGURATION – IPv4	16
Configuring PC in Windows 7 (IPv4)	16
Configuring PC in Windows Vista (IPv4)	18
Configuring PC in Windows XP (IPv4)	20
Configuring PC in Windows 2000 (IPv4)	21
Configuring PC in Windows 98/ME	22
Configuring PC in Windows NT4.0	23
NETWORK CONFIGURATION – IPv6	24
Configuring PC in Windows 7 (IPv6)	24
Configuring PC in Windows Vista (IPv6)	26
Configuring PC in Windows XP (IPv6)	28
DEFAULT SETTINGS	29
INFORMATION FROM YOUR ISP	30
CHAPTER 4: BASIC CONFIGURATION	31

LOGIN TO YOUR DEVICE	31
STATUS.....	32
QUICK START	33
WAN	36
EWAN	36
<i>Dynamic IP Address (Obtain an IP Address Automatically)</i>	<i>36</i>
<i>Fixed IP Address.....</i>	<i>36</i>
<i>PPPoE</i>	<i>37</i>
3G/4G LTE.....	38
WLAN	39

CHAPTER 5: ADVANCED CONFIGURATION 42

LOGIN TO YOUR DEVICE	42
STATUS.....	44
Mobile Status	45
System Log	46
3G/4G-LTE Status.....	47
ARP Table	48
DHCP Table.....	48
System Log	49
Firewall Log	49
UPnP Portmap.....	50
QUICK START	51
CONFIGURATION.....	55
LAN (Local Area Network)	55
Ethernet	55
IP Alias.....	55
Wireless.....	56
Wireless Security	58
WPS.....	61
DHCP Server	70
WAN (Wide Area Network)	72
WAN Interface (EWAN).....	72
WAN Interface (3G / 4G).....	72
WAN Interface(Dual WAN)	73
WAN Profile.....	74

Main Port - EWAN	74
Main Port - 3G / 4G	77
System.....	81
Time Zone.....	81
Firmware Upgrade	82
Backup / Restore	84
Restart Router	84
User Management	85
Mail Alert	86
Firewall and Access Control	87
Packet Filter.....	88
MAC Filter.....	90
Intrusion Detection.....	91
Block WAN PING.....	93
URL Filter.....	93
QoS - Quality of Service.....	95
Quality of Service Introduction	95
QoS Setup.....	95
Virtual Server	100
Port Mapping	101
DMZ	103
Wake on LAN.....	105
Time Schedule	106
Advanced	107
Static Route	107
Static ARP.....	107
Dynamic DNS.....	108
Device Management	109
SIP_ALG	116
Port NAT	116
IGMP	117
SNMP Access Control.....	118
TR-069 Client.....	120
Remote Access.....	121

SAVE CONFIGURATION TO FLASH	122
--	------------

RESTART	123
----------------------	------------

LOGOUT.....	124
--------------------	------------

CHAPTER 5: TROUBLESHOOTING 125

Problems with the Router	125
--------------------------------	-----

Problem with LAN Interface125

Recovery Procedures.....126

APPENDIX: PRODUCT SUPPORT & CONTACT
.....127

CHAPTER 1: INTRODUCTION

Introduction to your Router

Thank you for purchasing the **BEC 6200WZL (3G/4G_LTE Cellular Broadband Router)**. The router is an economic router ideal for SOHO users, office users and event organizers to have an improved wireless access with a speed of up to 150 Mbps. You can enjoy non-stop wireless access with this economic mobile 3G / 4G embedded router. With Dual-WAN design, you can also have an always-on WAN connection.

Always on Connection

The **BEC 6200WZL (3G/4G_LTE Cellular Broadband Router)** features dual-WAN interface allowing users to connect to the Internet via either wired connectivity of broadband device by plugging into a WAN port, or via 3G / 4G connections via inserting a 3G / 4G SIM card into its built-in SIM slot. The auto fail-over feature ensures maximum connectivity and minimum interruption by quickly and smoothly connecting to a 3G / 4G network in the event that your broadband Ethernet line fails. The router will then automatically reconnect to the broadband connection when it's restored, minimizing connection costs. These features are perfect for office situations where constant connection is paramount.

Mobility

With the increasing popularity of 3G / 4G standard, communication via **BEC 6200WZL (3G/4G_LTE Cellular Broadband Router)** is becoming more convenient and wide-available-allowing you to watch movies, download music on the road, run media-intensive application, or access e-mail with your client, team members, friends or family no matter where you are. You can even share your internet with others, whether you're in a meeting or speeding across the country on a train. The router can even function as a FTP server for network device sharing. The integrated wireless technology allows wireless access up to 150Mbps. The **BEC 6200WZL (3G/4G_LTE Cellular Broadband Router)** is truly free and mobile.

Upgraded Wireless Access and Security

With an integrated Wireless-N Access Point that supports up to 150Mbps wireless operation rate, yet it can switch compliance with 802.11b/g network devices. Wireless Protected Access (WPA-PSK / WPA2-PSK) and Wired Equivalent Privacy (WEP) features enhance the level of transmission security and access control over your Wireless LAN. If the network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows users to expand the wireless network without the need for any external wires or cables. Built-in with Stateful Packet Inspection (SPI), it enables users to determine whether a data packet is allowed to pass through the firewall to the private LAN. QoS Control prioritizes the traffic and allows users to enjoy smooth traffic flow while running applications such as P2P or multimedia through the Internet.

3G / 4G Management Center

With the **BEC 6200WZL (3G/4G_LTE Cellular Broadband Router)**, monitoring your 3G / 4G connection status is a breeze. Unique 3G / 4G Management Center is a utility tool displaying its current 3G / 4G-signal status visually for users to maximize their connection. You can monitor the

bandwidth with the current upload and download speed. This too also calculates the total amount of hours or data traffic used per month, allowing you to manage your 3G / 4G monthly subscriptions.

Features & Specifications

- 3G / 4G embedded with a built-in SIM card slot
- Dual WAN interfaces for EWAN and 3G / 3.5G / 3.75G / 4G connections
- 150Mbps. Wireless-N AP
- Supports Wi-Fi Protected Setup (WPS) and WPA-PSK / WPA2-PSK
- Supports multiple SSIDs for flexibility of network infrastructure
- High-speed wireless connection up to 150Mbps data rate
- Auto fail-over for always-on connection
- 3G / 4G Management Center for connection monitoring
- SOHO firewall security with DoS prevention and SPI
- Quality of Service control
- Syslog monitoring
- Ideal for SOHO users, Office users, and Event or meeting organizers

Available and Resilience

- Dual-WAN ports (3G / 4G & Ethernet WAN)
- Auto fail-over/fail-back

Network Protocols and Features

- NAT, static routing and RIP-1 / 2
- NAT supports PAT and multimedia applications
- Transparent bridging
- Virtual server and DMZ
- SNTP, DNS relay and DDNS
- IGMP snooping and IGMP proxy

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- Prevents DoS attacks including Land Attack, Ping of Death, etc.
- Remote access control for web base access
- Packet and URL filtering
- Password protection for system management
- VPN pass-through

Quality of Service Control

- Supports the DiffServ approach
- Traffic prioritization based-on IP protocol, port number and address

Wireless LAN

- Compliant with IEEE 802.11g and 802.11b standards
- 2.4GHz - 2.484GHz frequency range
- Up to 150Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless Security with WPA-PSK / WPA2-PSK support
- WDS repeater function support
- Multiple SSID

Management

- 3G / 4G Management Center
- Quick Installation Wizard
- Web-based for remote and local management
- Firmware upgrades and configuration data upload / download via web-based interface
- Embedded Telnet server for local management
- SNMP v1 / v2 / v3, MIB-I and MIB-II support
- System Log monitoring
- Supports DHCP server / client / relay
- Mail Alert

Hardware Specifications

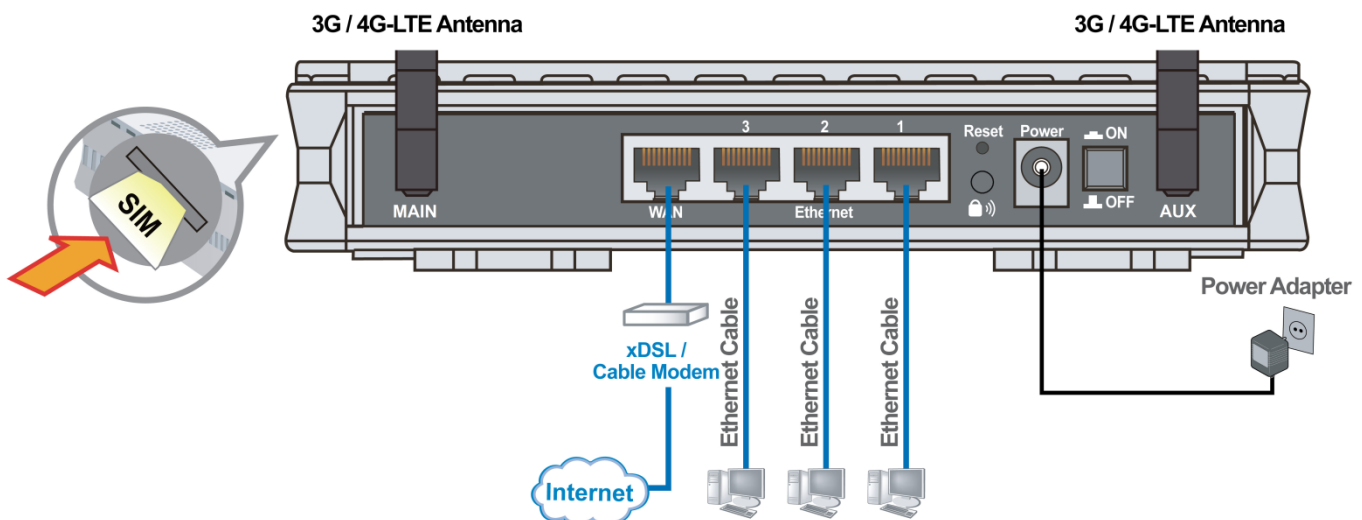
Physical interface

- 3G / 4G: 2 antennas
- Ethernet: 4 x 10 / 100Mbps Auto-MDI / MDI-X RJ-45 Ethernet ports
- WAN: 1 x 10 / 100Mbps Auto-MDI / MDI-X RJ-45 Ethernet port (port #4 can be configured as WAN port for Broadband connectivity.)
- Reset button
- WPS push button
- Power jack
- Power switch
- SIM slot : (for the SIM card from Telco / ISP)

Physical Specifications

- Dimensions: 7.28" x 4.86" x 1.38"(185mm x 123.5mm x 35mm)

Application Diagram



Attention

Connect the detachable 3G/4G-LTE antennas to the two jacks on the back of the device and make sure they are firmly screwed in. The MAIN antenna connector is used for primary 3G/4G-LTE. If deciding to use ONE antenna, make sure the MAIN antenna connector is being connected at all times.

CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router



Warning

- ✓ Do not use the router in high humidity or high temperature.
- ✓ Do not use the same power source for the BEC 6300VNL on other equipment.
- ✓ Do not open or repair the case yourself. If the device becomes too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ Avoid using this product and all accessories outdoors.

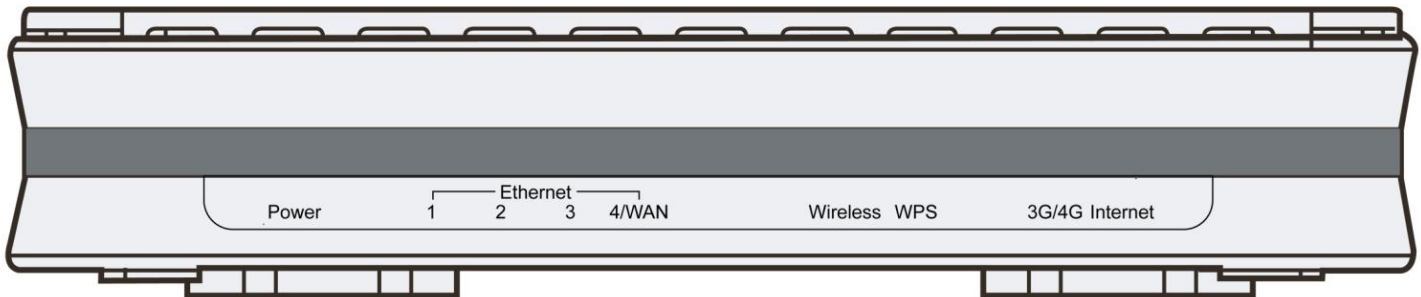


Attention

- ✓ Place the router on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

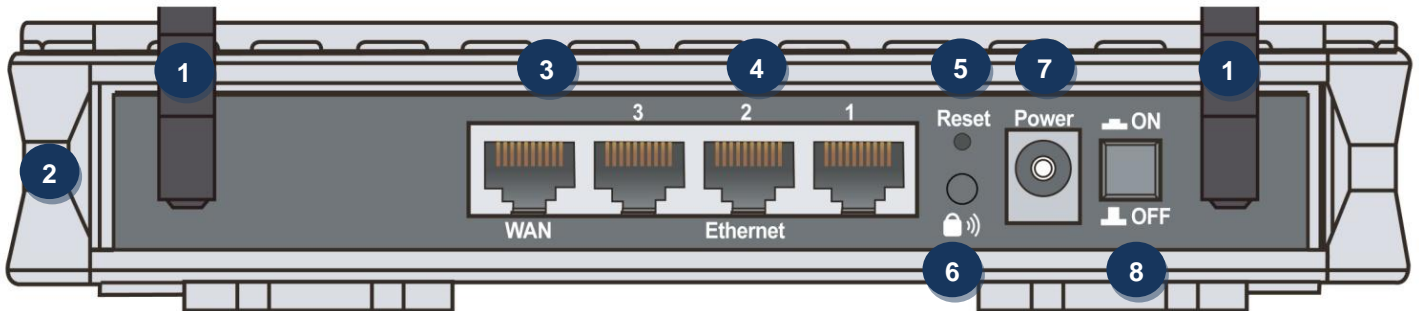
Device Description



Front Panel LEDs



LED	STATUS	DESCRIPTION
Power	Green	System is up and ready
	Red	Boot failure
Ethernet Port LAN 1 ~ 4	Green	LAN Port is connected to an Ethernet unit, e.g. PC, Notebook, Xbox
	Blinking	Data being transmitted/received
	Note: port #4 can be configured as WAN port for broadband connectivity	
EWAN on LAN 4	Green	BEC 6200WZL is successfully connected with a broadband connection device.
	Blinking	Data being transmitted/received
Wireless	Green	Wireless connection established
	Blinking	Data being transmitted / received
WPS	Green	Wireless client has been connected via WPS successfully
	Blinking	WPS is enabled and ready for other wireless clients to join
3G/4G (Received Signal Strength Indicator)	Green	RSSI greater than -69 dBm. Excellent signal condition
	Green Flashing quickly	RSSI from -81 to -69 dBm. Good signal condition
	Orange Flashing quickly	RSSI from -99 to -81 dBm. Fair signal condition.
	Orange Flashing slowly	RSSI less than -99 dBm. Poor signal condition.
	Orange	No signal and the 4G_LTE module is in service
	Off	No LTE module or LTE module fails
Internet	Green	WAN IP received and traffic is passing thru the device.
	Red	WAN IP request failed.
	Off	BEC 6200WZL is either in bridged mode or WAN connection not ready.

Rear Panel Connectors



PORT		MEANING
1	LTE Antenna	Screw the supplied LTE antennas onto the antenna connectors on both sides.
2 	SIM Card Slot	Insert the mini SIM card (2FF) with the gold contact facing down. Push the mini SIM card (2FF) inwards to eject it
3	WAN	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps /100Mbps.
4	Ethernet LAN (1~4)	Connect to Fiber/ Cable/ xDSL Modem with a RJ-45 cable WAN Port (LAN port 4) can also be a regular Ethernet LAN port.
5	Reset	After the device is powered on, press it 6 seconds or above : to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot your password)
6 	WPS & Wireless On/Off	By controlling the pressing time, users can achieve two different effects: (1) WPS^{*1} : Press &hold the button for less than 6 seconds to trigger WPS function. (2) Wireless ON/OFF button : Press & hold the button for more than 6 seconds to On/Off the wireless.
7	Power Jack (DC)	Connect the supplied Power Adapter to this jack.
8	Power Switch	Power ON/OFF switch

* Note: 1. For WPS configuration, please refer to the WPS section in the User Manual.

Cabling

One of the most common causes of problems is bad cabling. Make sure that all connected devices are turned on. On the front panel of the product is a bank of LEDs. Verify that the LAN Link and LEDs are lit. If they are not, verify that you are using the proper cables.

Make sure that all other devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your BEC router have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If the line filter is not correctly installed and connected, it may cause problems to your connection or may result in frequent disconnections.

CHAPTER 3: BASIC INSTALLATION

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Windows 98 / NT / 2000 / XP / ME / 7 / Vista, Linux, Mac OS, etc. The product provides an easy and user-friendly interface for configuration.

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and have TCP/IP installed or configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.1.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

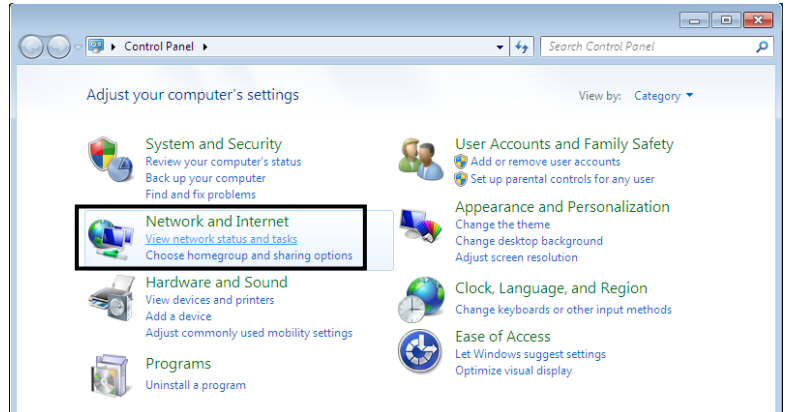


Any TCP/IP capable workstation can be used to communicate with or through the BEC 6200WZL. To configure other types of workstations, please consult the manufacturer's documentation.

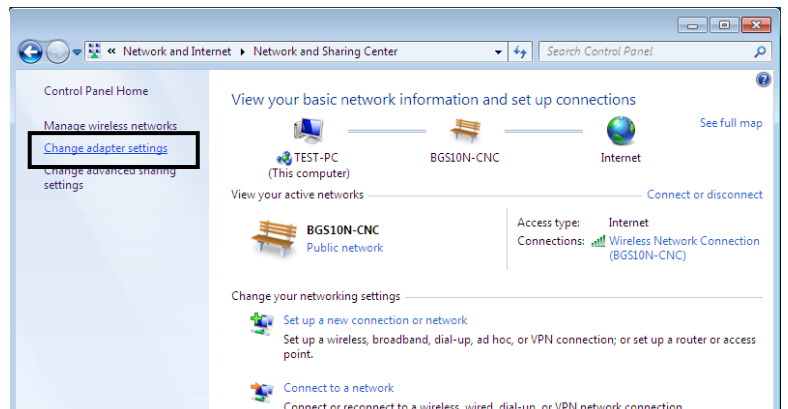
Network Configuration – IPv4

Configuring PC in Windows 7 (IPv4)

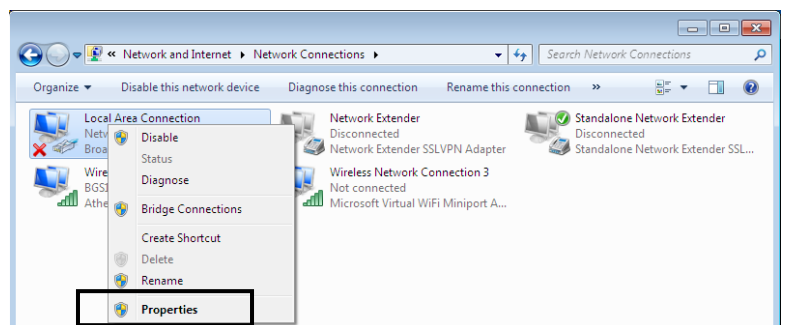
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



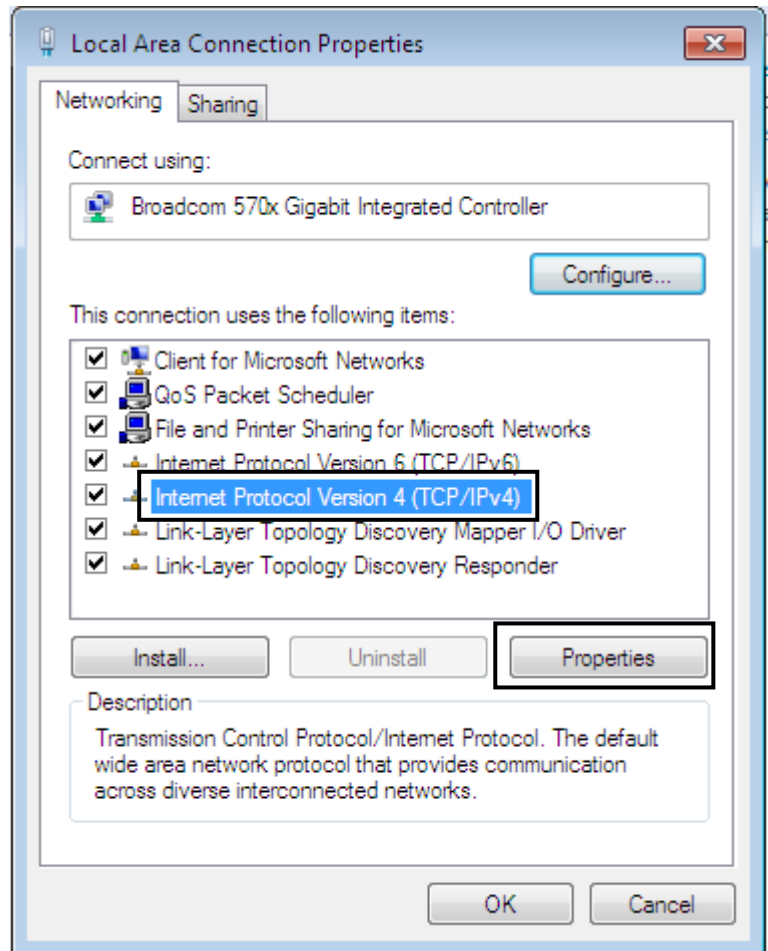
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



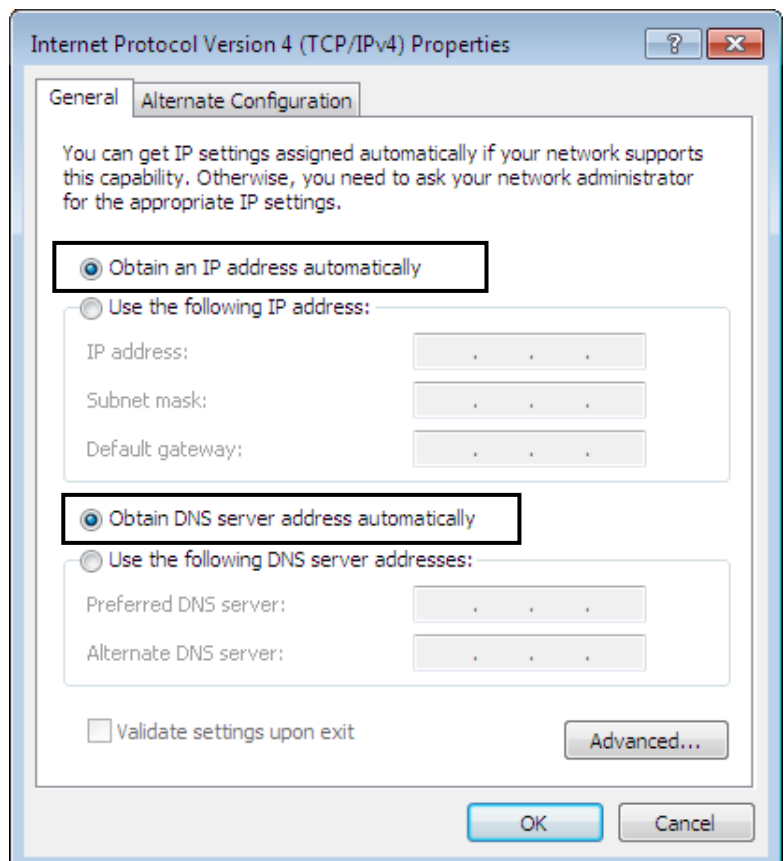
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.

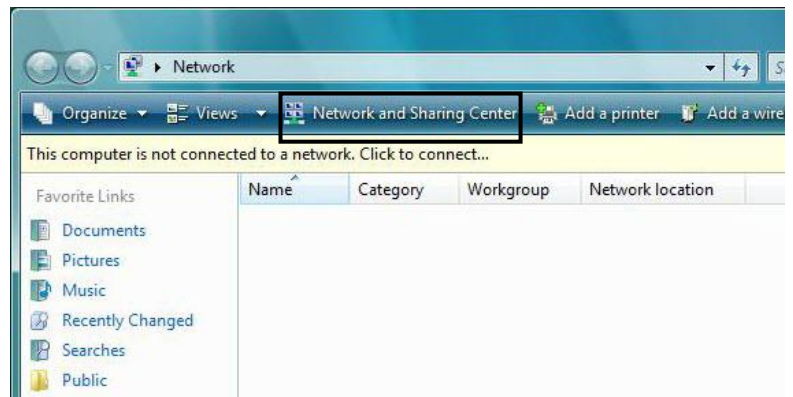


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv4)

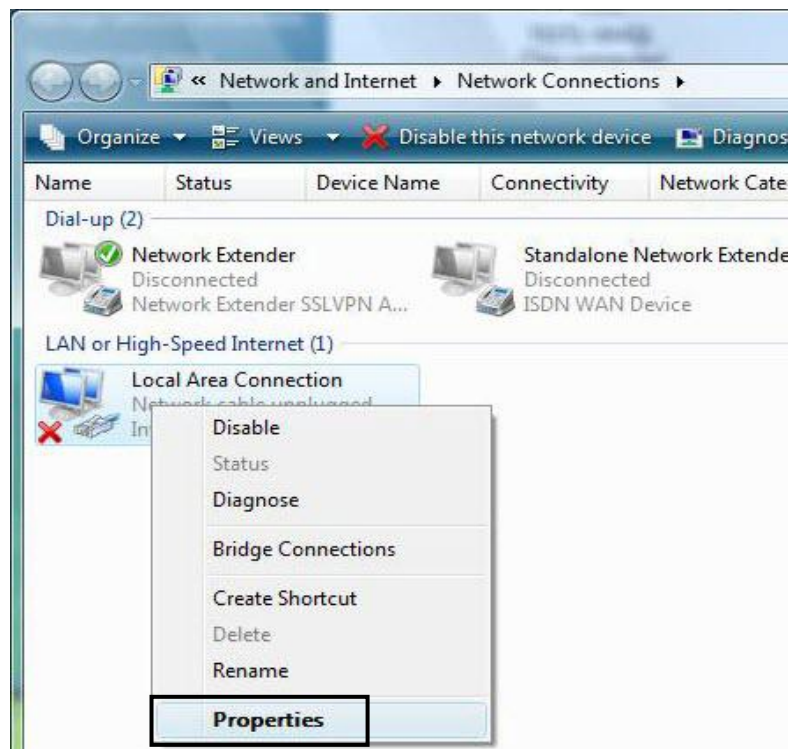
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



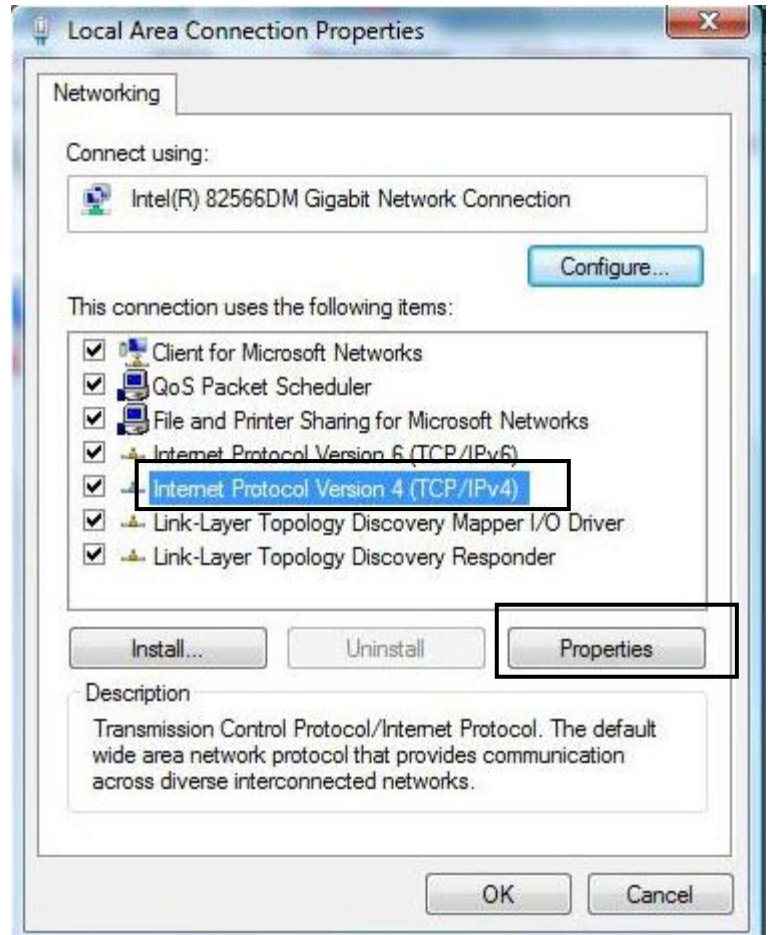
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

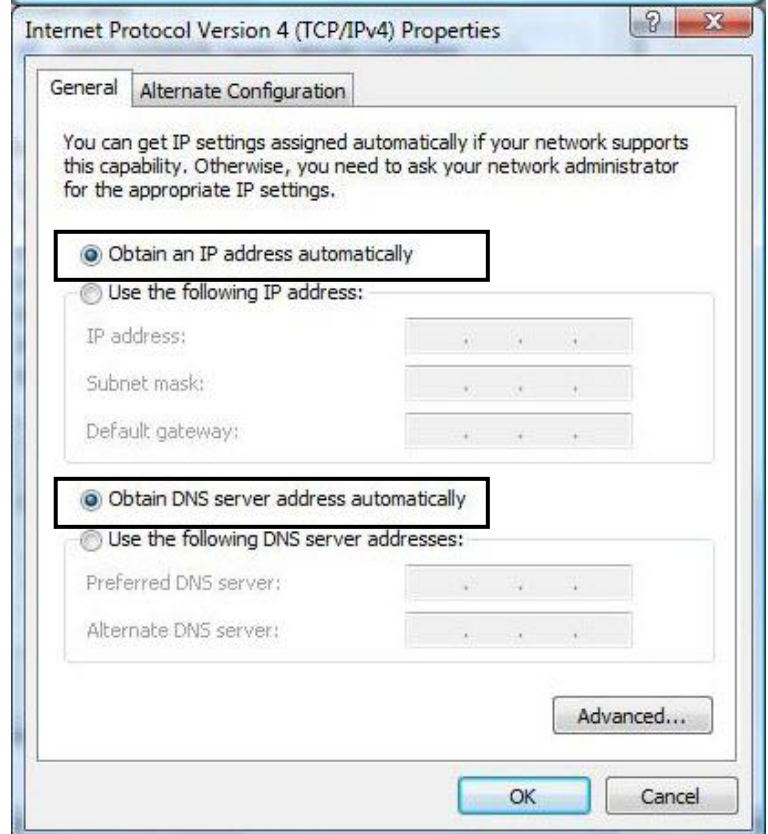


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



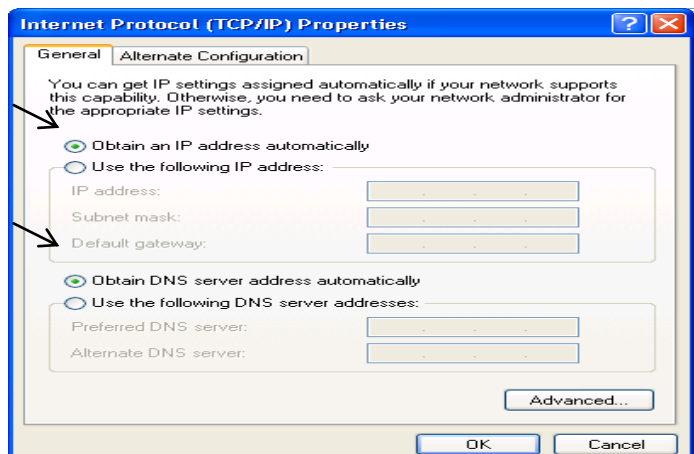
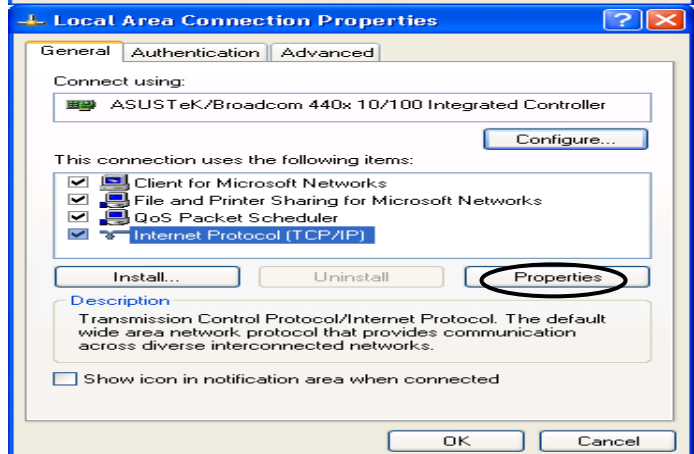
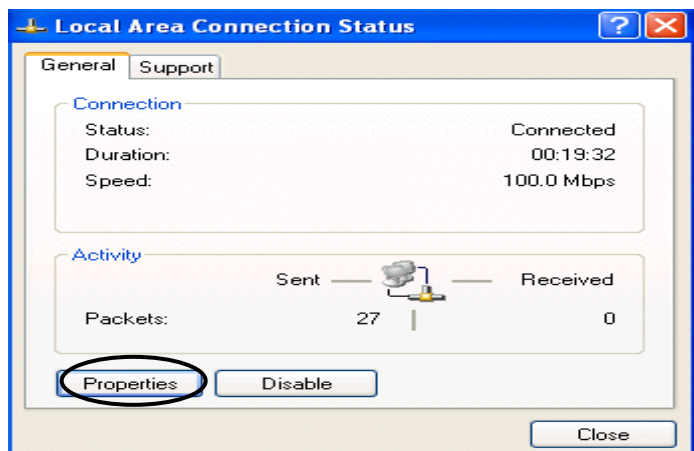
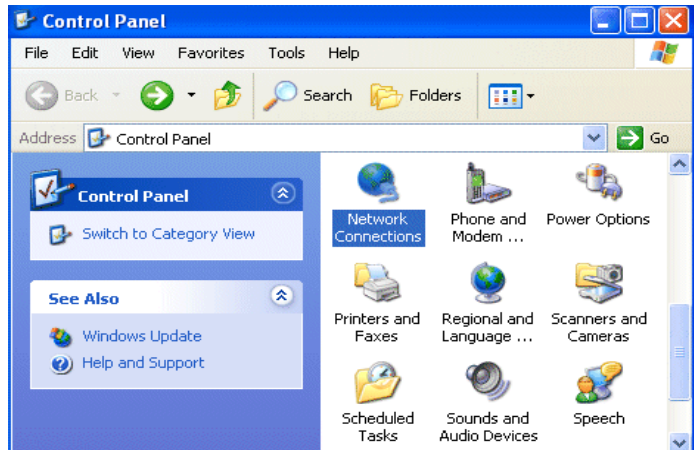
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows XP (IPv4)

1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.
3. In the **Local Area Connection Status** window, click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.



Configuring PC in Windows 2000 (IPv4)

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.

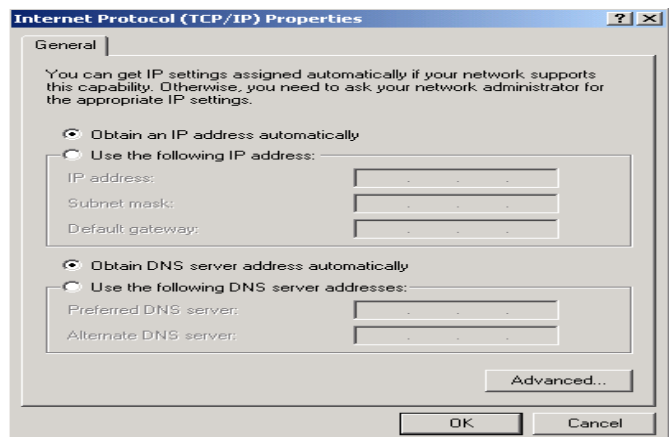
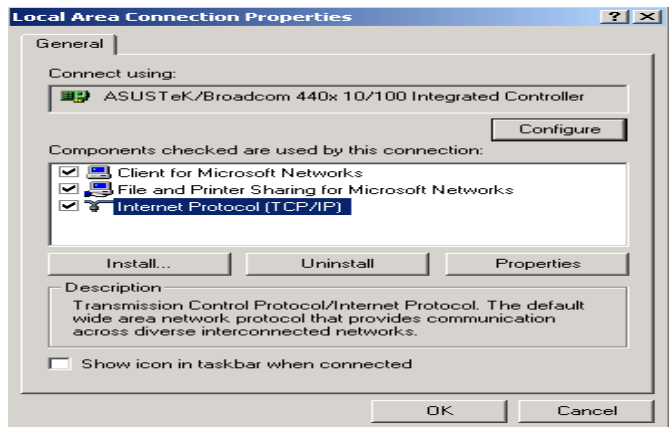
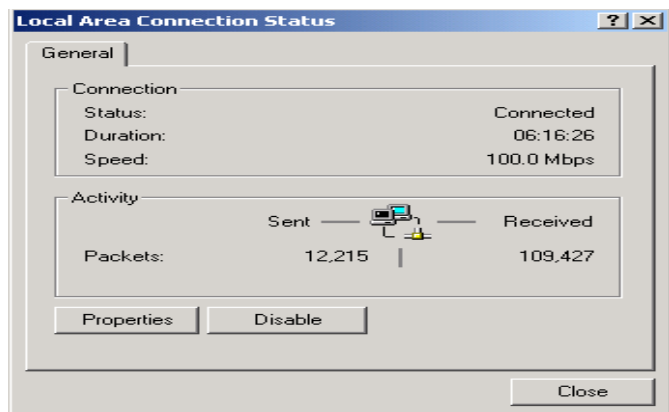
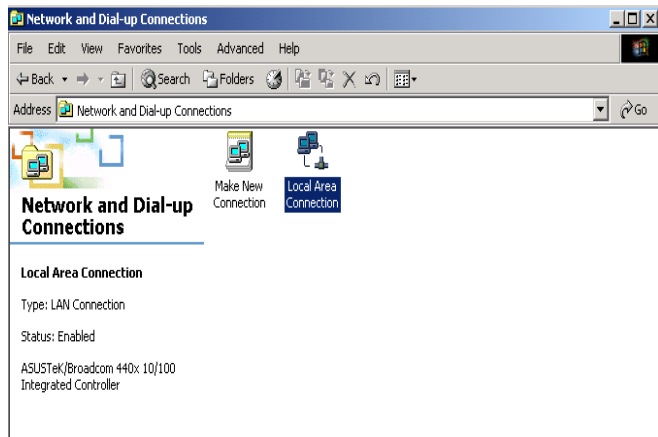
2. Double-click **Local Area Connection**.

3. In the **Local Area Connection Status** window click **Properties**.

4. Select **Internet Protocol (TCP/IP)** and click **Properties**.

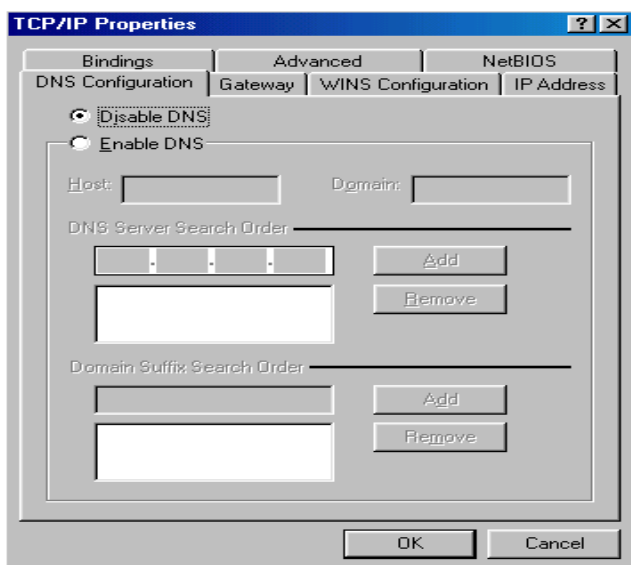
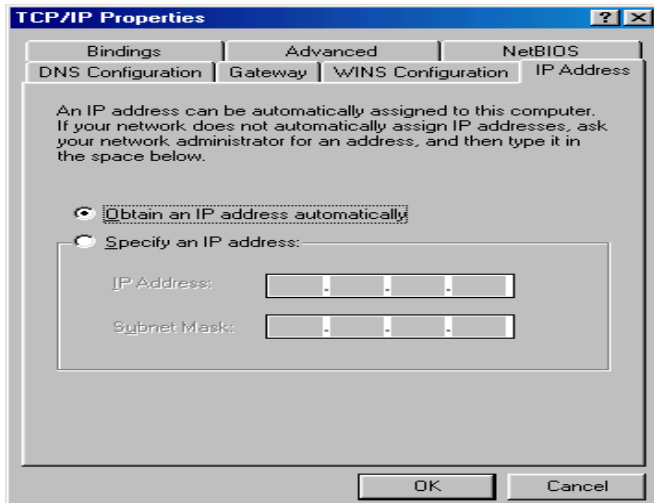
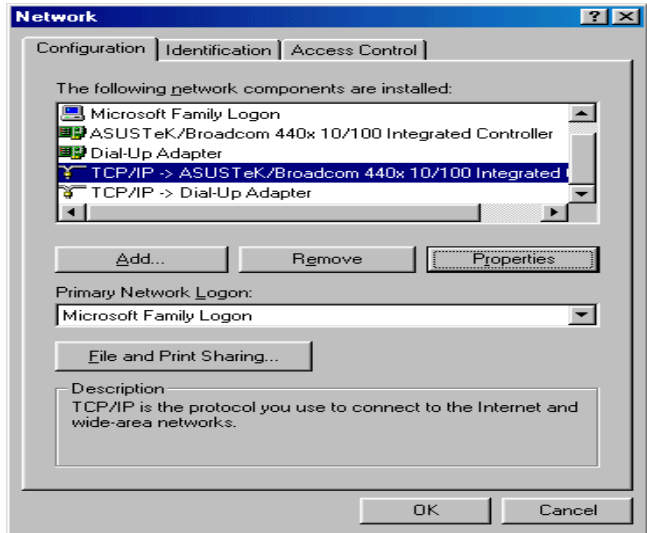
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.



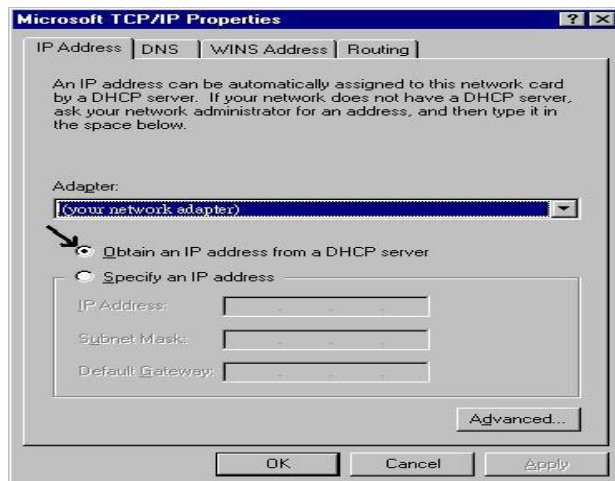
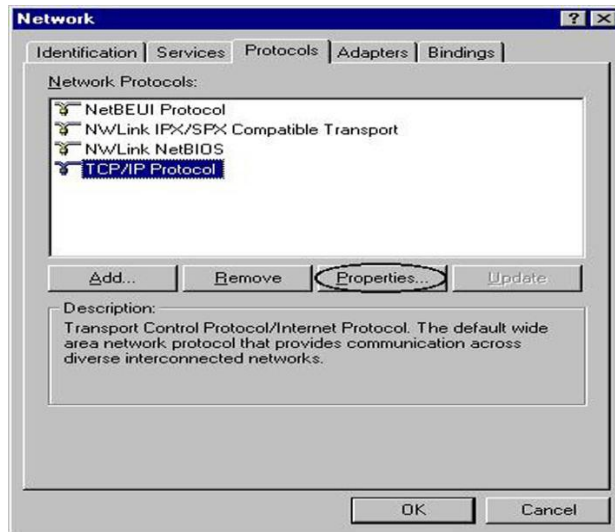
Configuring PC in Windows 98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP/IP ->NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.
3. Select the **Obtain an IP address automatically** radio button.
4. Then select the **DNS Configuration** tab.
5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



Configuring PC in Windows NT4.0

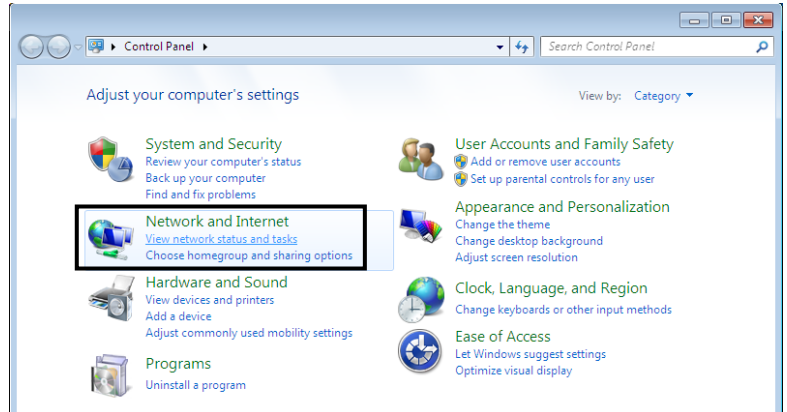
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.
3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



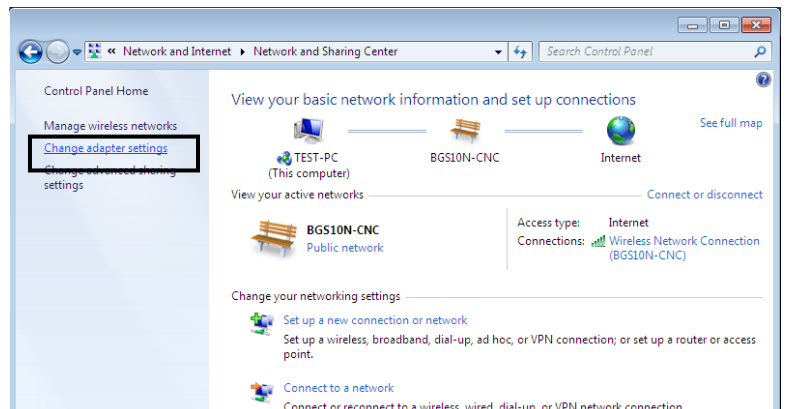
Network Configuration – IPv6

Configuring PC in Windows 7 (IPv6)

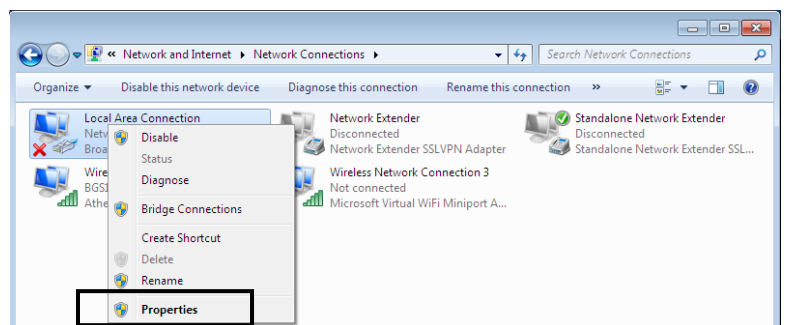
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



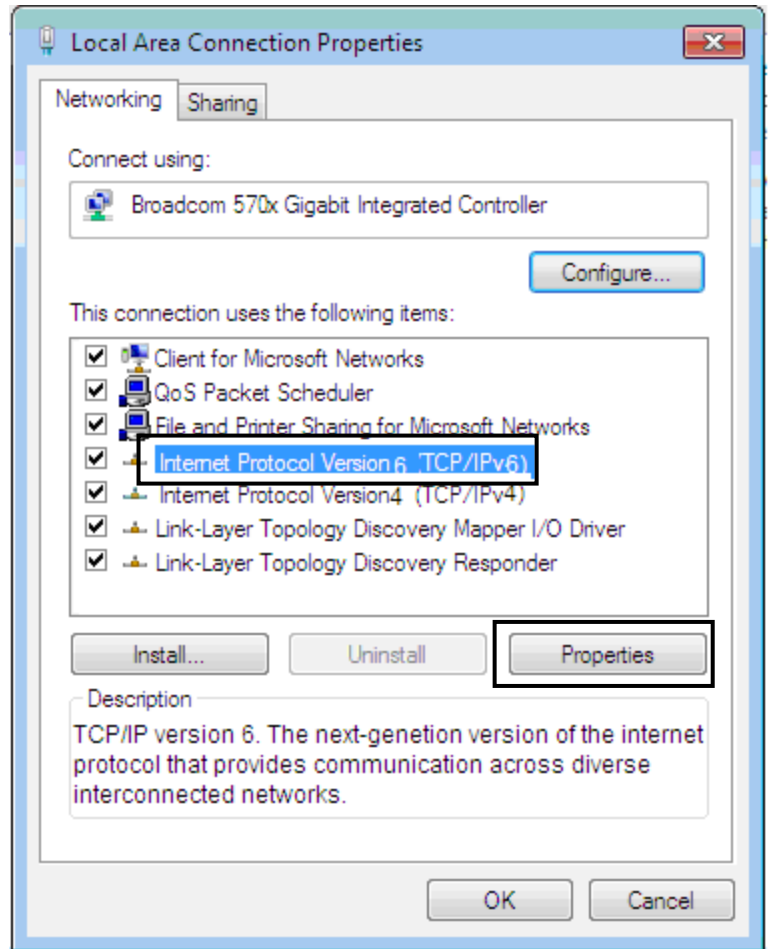
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



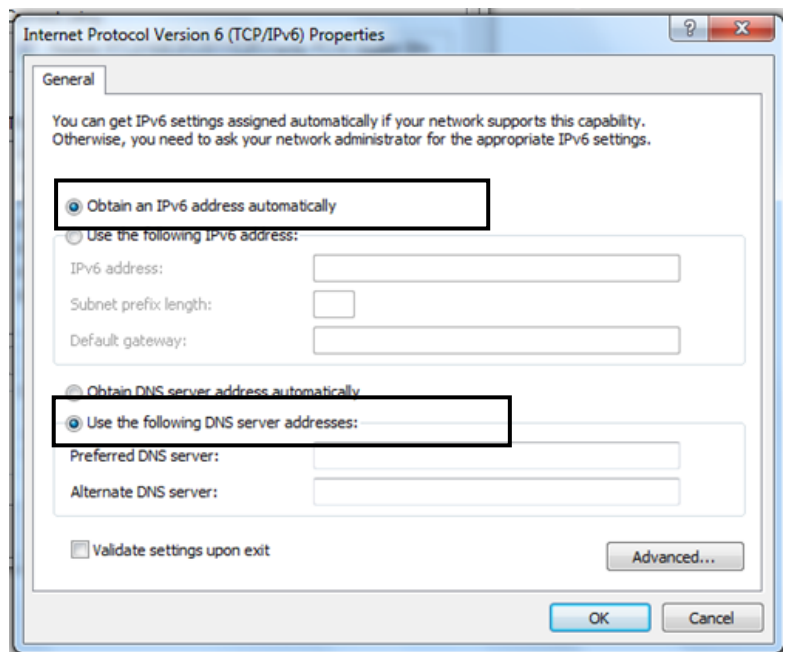
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.

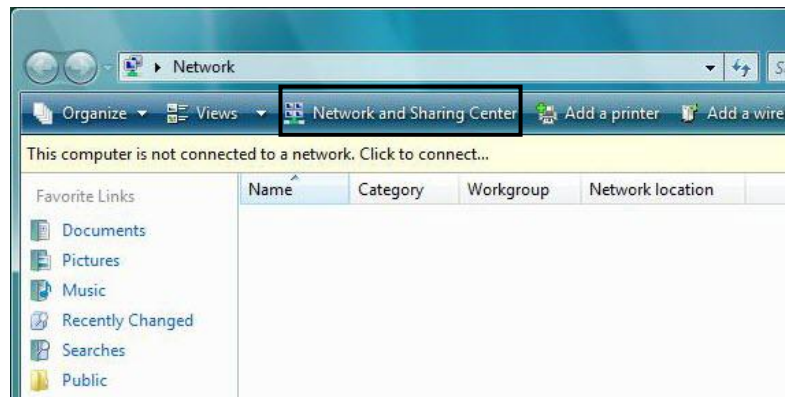


6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv6)

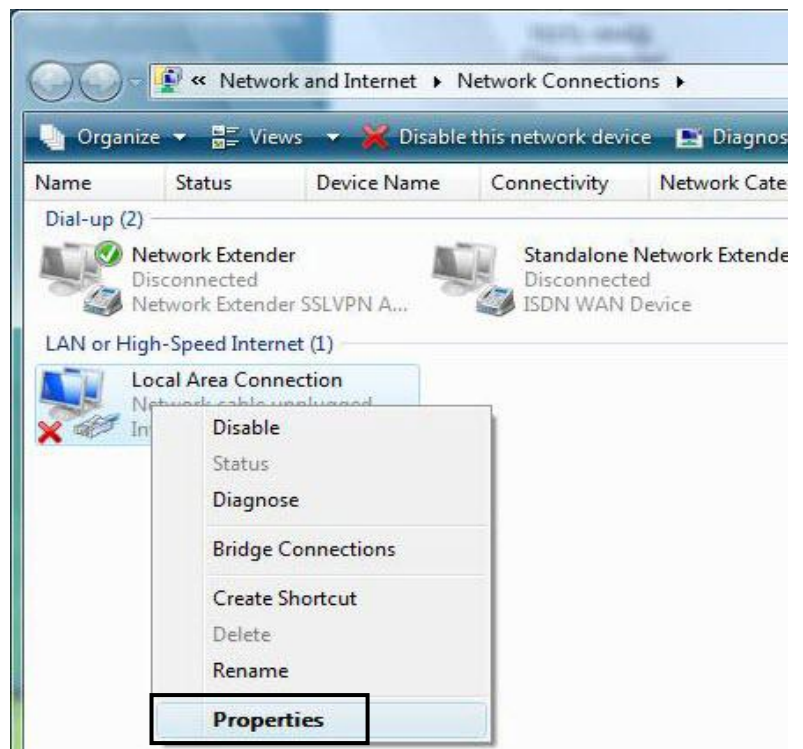
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



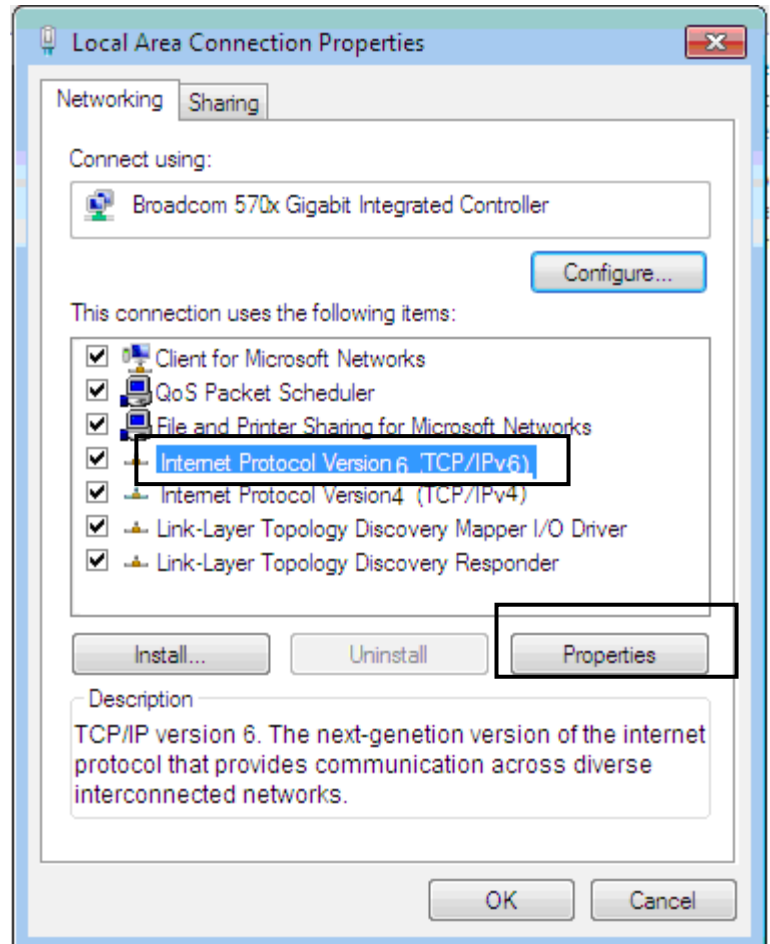
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

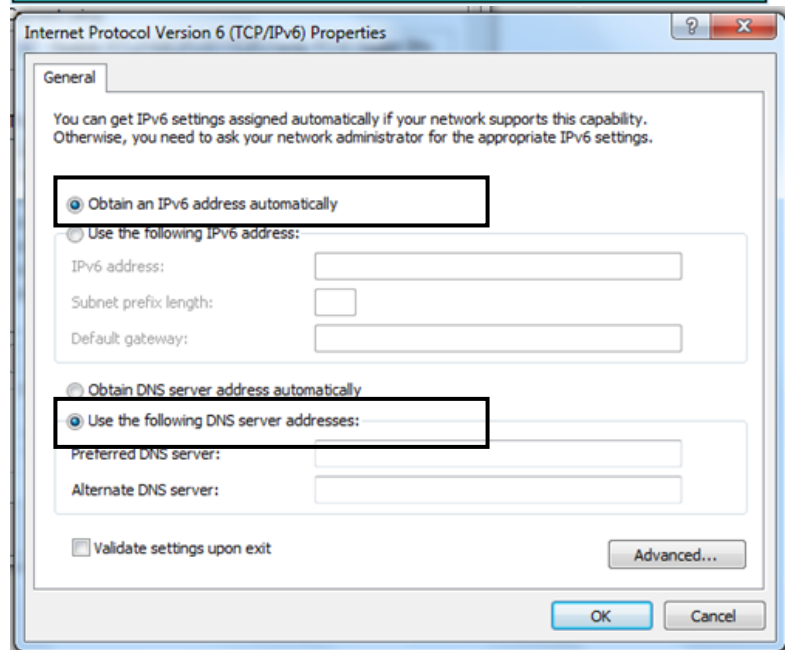


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



6. In the **TCP/IPv6 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

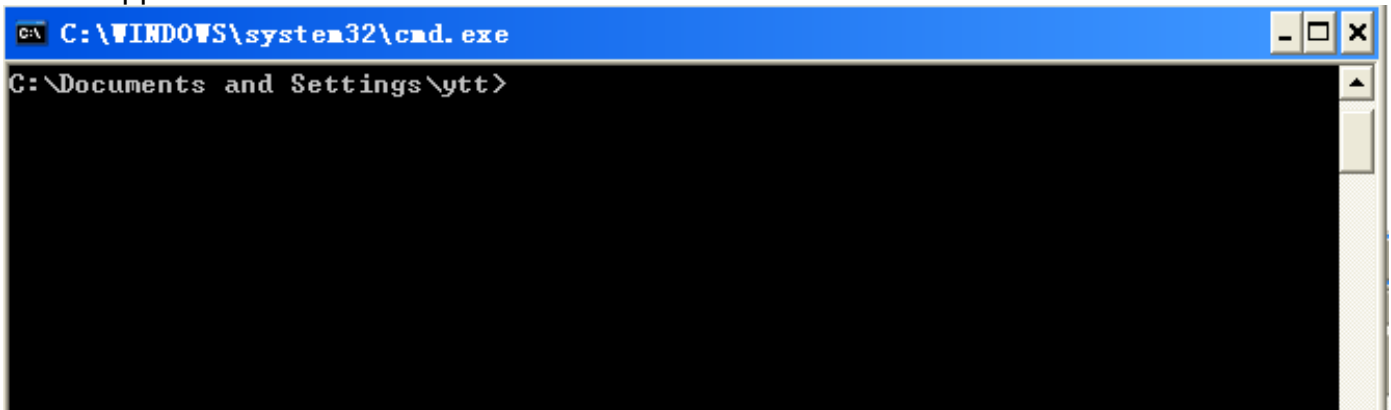


Configuring PC in Windows XP (IPv6)

IPv6 is supported by Windows XP, but you need to install it first.

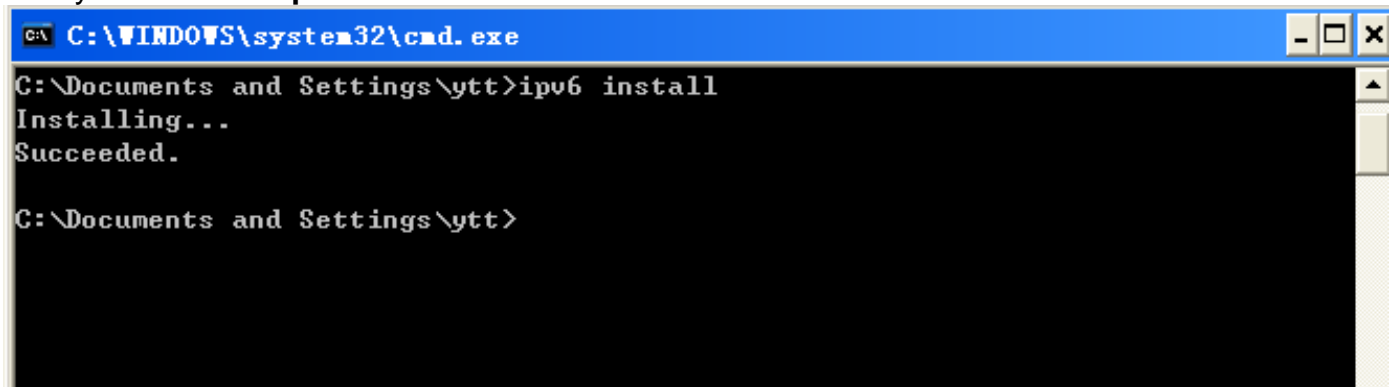
Please follow the steps to install IPv6:

1. On the Desktop, Click **Start > Run**, type **cmd**, then press **Enter** key in the keyboard, the following screen appears.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>
```

2. Key in command **ipv6 install**



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>ipv6 install
Installing...
Succeeded.
C:\Documents and Settings\ytt>
```

Installation of IPv6 is now completed. Please test it to see if it works or not. .

Default Settings

Before configuring the router, you need to know the following default settings.

Web Interface: (Username and Password)

- ✓ Username: admin
- ✓ Password: admin

The default username and password are “**admin**” and “**admin**” respectively.



If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

Device LAN IP Settings

- ✓ IP Address: 192.168.1.254
- ✓ Subnet Mask: 255.255.255.0

DHCP Server:

- ✓ DHCP server is enabled.
- ✓ Start IP Address: 192.168.1.100
- ✓ IP pool counts: 100

Information from Your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as **EWAN** ((Dynamic IP address, Static IP address, PPPoE, Bridge Mode).

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
Dynamic IP Address	DHCP Client (it can be automatically assigned by your ISP when you connect or be set manually).
Static IP Address	IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).
Bridge Mode	Pure Bridge

CHAPTER 4: BASIC CONFIGURATION

Login to your Device

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click “**Go**”, a user name and password window prompt appears.

The default username and password is “**admin**” and “**admin**” respectively for the **Administrator**.

NOTE: This username / password may vary by different Internet Service Providers.



Mobile Broadband Wireless-N Router

Username:

Password:

Account Type:

Login

Congratulations! You have successfully logged on to your BEC 6200WZL.

Once you have logged on to your 6200WZL via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

- 🌐 **Advanced** (Click to switch to the Advanced Configuration Mode)
- 🌐 **Status**
- 🌐 **Quick Start**
- 🌐 **WAN (EWAN, 3G/4G_LTE)**
- 🌐 **WLAN**

Status

Status

Device Information

Model Name6200WZLR4-A

System Up-Time29 min(s)

Software Version1.06.r8

Port Status

Ethernet✓

EWAN✗

3G/4G✓

Wireless▶✓

WAN

Port▶	Protocol	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
3G/4G		Disconnect	00:28:12	172.17.90.175	255.255.255.224	172.17.90.161	58.240.57.33
3G/4G			Connected	172.17.128.54	255.255.255.255	10.64.64.64	58.240.57.33

Device Information

Model Name: Name of the router for identification purpose.

Firmware Version: Software version currently loaded in the router

MAC Address: A unique number that identifies the router

Port Status

Port Status : User can look up to see if they are connected to Ethernet, EWAN, 3G / 4G and Wireless.

WAN

Port: Name of the WAN connection.

Protocol: PPPoE, Dynamic or Fixed for WAN

Operation: Current available operation.

Connection: The current connection status.

IP Address: WAN port IP address.

Netmask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

Primary DNS: The IP address of the primary DNS server.

Quick Start

The Quick Start Wizard is a helpful guide for the first-time users to the device and will guide you step by step to setup your BEC 6200WZL device.

Step 1 – Time Zone

Choose your time zone. Click **NEXT** to continue.

The screenshot shows the 'Quick Start' wizard interface. Under the 'Time Zone' section, there are two radio buttons: 'Enable' (selected) and 'Disable'. Below them is a dropdown menu for 'Local Time Zone (+GMT Time)' with the selected value '(GMT-06:00) Central Time (US & Canada)'. At the bottom of the section is a 'Continue' button.

Step 2 – WAN

Set up your Internet connection.

Select an appropriate WAN connection mode then click **Continue** to the next step.

To skip the WAN setting, click "**Jump to Wireless Setting**" to setup local wireless network.

The screenshot shows the 'Quick Start' wizard interface for the 'WAN Port' section. It has a breadcrumb 'WAN > Wireless'. The 'Select WAN Port' section contains a 'Connect Mode' dropdown set to 'EWAN (Recommended)' and a 'Protocol' dropdown set to 'Obtain an IP Address Automatically'. At the bottom are 'Continue' and 'Jump to Wireless setting' buttons.

2.1 If selected **EWAN / Obtain an IP Address Automatically**

Simply click on the **Apply** button to continue to the next step.

The screenshot shows the 'Configuration' screen for the 'WAN Port' section. It has a breadcrumb 'WAN Port'. Under 'WAN Connection', the 'Main Port' dropdown is set to 'EWAN' with a note '(Current Main Port : EWAN)'. Under 'Parameters', the 'Protocol' dropdown is set to 'Obtain an IP Address Automatically'. At the bottom are 'Apply' and 'Cancel' buttons.

2.2 If selected **EWAN / Fixed IP Address** (for example).

Please manually enter the assigned WAN IP information provided by your ISP. Click on Apply to continue.

Configuration

▼ WAN Port

WAN Connection

Main Port: EWAN (Current Main Port: EWAN)

Parameters

Protocol: Fixed IP Address

IP Address: 0.0.0.0

Netmask:

Gateway:

Apply Cancel

2.3 If selected **EWAN / PPPoE**

Please enter PPPoE account information provided by your ISP. Click on Apply to continue

Configuration

▼ WAN Port

WAN Connection

Main Port: EWAN (Current Main Port: EWAN)

Parameters

Protocol: PPPoE

Username:

Password:

Service Name:

IP Address: 0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')

Authentication Protocol: Auto

Apply Cancel

2.4 If selected **3G/4G-LTE**

Input all relevant 3G/4G-LTE parameters from your ISP.

Quick Start

▼ WAN Port

WAN Connection

Main Port: 3G/4G (Current Main Port: 3G)

Parameters

ISP Mode: AT&T_US

TEL No.: *99***1#

APN: internet

Username:

Password:

Authentication Protocol: Auto

PIN:

*Warning: Entering the wrong PIN code three times will lock the SIM.

Apply Cancel

Note: when re-inserting the 3G / 4G SIM card to the BEC 6200WZL, you should again press **Apply** button to make 3G / 4G connection take effort, or you can Save Config and Restart the router to reach the same effort.

Step 3 – Wireless

Set up your wireless connection if you want to connect to the Internet wirelessly on your PCs. Click on Continue to the next step

Quick Start

▼ Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
Channel ID	Auto
Security Mode	WPA/WPA2 Pre-Shared Key
Regulation Domain	N.America
WPA Shared Key	0004ED012340

Continue

Step 4 – Saving Configuration

Quick Start

▼ Save configuration

Saving configuration to FLASH. Please wait for 10 seconds

Step 5 – Quick Start Completed!

You now may be able to access to the Internet. If not, please check your WAN, Internet Connection, setup again.

Quick Start

▼ Process finished

Success.

The Quick Start process is finished. Your device has been successfully configured.

WAN

EWAN

Dynamic IP Address (Obtain an IP Address Automatically)

No additional configuration is required. Click “Apply” to save the settings. BEC 6200WZL will request then obtain IP address automatically.

The screenshot shows the 'Configuration' tab of the WAN settings. Under the 'WAN Port' section, the 'WAN Connection' is set to 'EWAN'. The 'Main Port' is also 'EWAN', with a note '(Current Main Port : EWAN)'. Under the 'Parameters' section, the 'Protocol' is set to 'Obtain an IP Address Automatically'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Fixed IP Address

Select this option to set static IP information. You will need to enter in the Connection type, IP address, Netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four IP octets separated by a dot (xx.xx.xx.xx). The Router will not accept the IP address if it is not in this format.

The screenshot shows the 'Configuration' tab of the WAN settings. Under the 'WAN Port' section, the 'WAN Connection' is set to 'EWAN'. The 'Main Port' is also 'EWAN', with a note '(Current Main Port : EWAN)'. Under the 'Parameters' section, the 'Protocol' is set to 'Fixed IP Address'. Below this, there are input fields for 'IP Address' (containing '0.0.0.0'), 'Netmask', and 'Gateway'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Protocol: The current ATM protocol in the device

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

Netmask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0. Type the subnet mask assigned to you by your ISP (if given).

Gateway: You must specify a gateway IP address (supplied by your ISP)

PPPoE

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.

The screenshot shows a web-based configuration interface for a WAN Port. The 'Configuration' tab is active. Under the 'WAN Port' section, the 'WAN Connection' is set to 'EWAN'. The 'Parameters' section includes: 'Protocol' set to 'PPPoE', 'Username' and 'Password' fields, 'Service Name' field, 'IP Address' set to '0.0.0.0' with a note that it means 'Obtain an IP address automatically', and 'Authentication Protocol' set to 'Auto'. 'Apply' and 'Cancel' buttons are at the bottom.

Configuration	
▼ WAN Port	
WAN Connection	
Main Port	EWAN (Current Main Port : EWAN)
Parameters	
Protocol	PPPoE
Username	
Password	
Service Name	
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Auto
Apply Cancel	

Protocol: The current ATM protocol in the device

Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).

Service Name: Enter a name for this connection.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is in Auto mode which the setting will be assigned by your ISP either using a Chap or Pap.

3G/4G LTE

(The router also support 4G network, and user must tell the provider the exact 4G service you want for the 4G router)

Quick Start

▼WAN Port

WAN Connection

Main Port

3G/4G ▼ (Current Main Port : 3G)

Parameters

ISP Mode

AT&T_US ▼

TEL No.

*99***1#

APN

internet

Username

Password

Authentication Protocol

Auto ▼

PIN

*Warning: Entering the wrong PIN code three times will lock the SIM.

Apply

Cancel

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS / LTE call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you access to the internet i.e. Some 3G / 4G operators use the APN 'internet' for their portal. The default value of APN is "broadband".

Username: Enter the username provided by your service provider.

Password: Enter the password provided by your service provider.

Authentication Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which authentication type the server is using (when acting as a client), or the authentication type you want the clients to use when they are connecting to you (when acting as a server). When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authentication. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and a PUK code will be required from your network / service provider to unlock it.

Note: when re-inserting your 3G / 4G SIM card, again press the Apply button again to make 3G / 4G connection take effort, or you can Save Config and Restart the router to reach the same effort.

WLAN

Configuration

WLAN

Wireless Parameters

WLAN Service

☒ Enable
 ☐ Disable

ESSID

wlan-ap

Hide ESSID

☐ Enable
 ☒ Disable

Regulation Domain

N.America

Channel ID

Channel 1 (2.412 GHz)

Security Parameters

Security Mode

WPAWPA2 Pre-Shared Key

WPA Shared Key

0004ED012340

Group Key Renewal

3600

seconds

Apply

Cancel

Wireless Parameters

WLAN Service: Default setting is set to **Disable**.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Note: ESSID is case sensitive and must not excess 32 characters.

Hide ESSID: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Disable**.

- **Enable:** Select Enable if you do not want broadcast your ESSID. When select **Enable**, the ESSID will be hidden instead of broadcasting, thus when wireless client searches for this AP, failure occurs. This ESSID (AP) will be invisible to you. In this case, if you want to join this wireless network, enter the exactly ESSID manually and some security settings.
- **Disable:** When Disable is selected, the router will broadcast the ESSID to allow anybody with a wireless client to be able to identify the Access Point (AP) of your router. Select the specific ESSID scanned, with some security settings, you will join this wireless network.

Regulation Domain: There are seven Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

Channel ID: Select the ID channel that you would like to use.

Security Parameters

Security Mode: To change this Wi-Fi security mode, please go to the Wireless_Security section under Advanced / LAN. If you login using a User account, please contact the Administrator to change this setting for you.

► WPA Pre-Shared Key

Security Parameters	
Security Mode	WPA Pre-Shared Key ▼
WPA Shared Key	0004ED012340
Group Key Renewal	3600 seconds

WPA Shared Key: The key for network authentication. The input format is in character style and the key size should be in the range between 8 and 63 characters (here the default is the router or CPE's MAC address in uppercase).

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

► WPA2 Pre-Shared Key

Security Parameters	
Security Mode	WPA2 Pre-Shared Key ▼
WPA Shared Key	0004ED012340
Group Key Renewal	3600 seconds

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters (here the default is the router or CPE's MAC address in uppercase).

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

► WPA / WPA2 Pre-Shared Key

Security Parameters	
Security Mode	WPA/WPA2 Pre-Shared Key ▼
WPA Shared Key	0004ED012340
Group Key Renewal	3600 seconds

WAP Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters (here the default is the router or CPE's MAC address in uppercase).

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

► WEP

Security Parameters	
Security Mode	WEP ▼
WEP Authentication	Open System ▼
Default Used WEP Key	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
Passphrase (Generate Key)	<input type="text"/> <input type="button" value="WEP64"/> <input type="button" value="WEP128"/>
Key 1	Hex ▼ <input type="text"/>
Key 2	Hex ▼ <input type="text"/>
Key 3	Hex ▼ <input type="text"/>
Key 4	Hex ▼ <input type="text"/>

WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33.
 WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
 WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33dd44ee55efffe35f.
 WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?!dbd3ert.

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are three options to select from: **Open System, Share key or Both.**

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the **Passphrase** is enabled.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively and no spaces allowed.

WPA Shared Key: The key for network authentication. The input format is in character style and the key size should be in the range between 8 and 63 characters (here the default is the router or CPE's MAC address in uppercase).

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

CHAPTER 5: ADVANCED CONFIGURATION

Login to your Device

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click **Go**, a user name and password window prompt appears. Enter the user name and password that your administrator has set for you and select the **Account Type**, then click **Login**.

The default username and password is **“admin”** and **“admin”** respectively for the **Administrator** account type.



Mobile Broadband Wireless-N Router

Username:

Password:

Account Type: Administrator ▼

Login

Congratulations! You have successfully logged on to your **BEC 6200WZL**.

Once you have logged on to your 6200WZL via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

Section	Status	Quick Start (Wizard Setup)	Configuration
Sub-Items	Mobile Status		LAN <ul style="list-style-type: none"> - Ethernet - IP Alias - Wireless - Wireless Security - WPS - DHCP Server
	USB Status		WAN <ul style="list-style-type: none"> - WAN Interface - WAN Profile
	ARP Table		System <ul style="list-style-type: none"> - Time Zone - Firmware Upgrade - Backup / Restore - Restart - User Management - Mail Alert
	DHCP Table		Firewall <ul style="list-style-type: none"> - Packet Filter - MAC Filter - Intrusion Detection - Block WAN Ping - URL Filter
	System Log		QoS
	Firewall Log		Virtual Server <ul style="list-style-type: none"> - Port Mapping - DMZ
	UPnP Portmap		Wake on LAN
			Time Schedule
			Advanced <ul style="list-style-type: none"> - Static Route - Static ARP - SIP_ALG - Port NAT - IGMP - SNMP Access Control - TR-069 Client - Remote Access

Please see the relevant sections of this manual for detailed instructions on how to configure your **BEC 6200WZL** gateway.

Status

In this section, you can check the router working status, including **Mobile Status**, **USB Status**, **ARP Table**, **DHCP Table**, **System Log**, **Firewall Log**, and **UPnP Portmap**.

Status

▼ Device Information

Model Name	Mobile Broadband Wireless-N Router
Host Name ▶	home.gateway
System Up-Time	11 min(s)
Current Time ▶	Fri Dec 7 13:04:20 2012
Software Version	1.05.dc9
MAC Address	00:04:ed:01:23:40

▼ Port Status

Ethernet	✓
EWAN	✗
3G/4G ▶	✓
Wireless ▶	✓

▼ WAN

Port ▶	Protocol	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
3G/4G ▶		<div>Disconnect</div>	00:09:33	172.26.44.229	255.255.255.252	172.26.44.230	58.240.57.33

Device Information

Model Name: Name of the router for identification purpose.

Host Name: Used as simple identification purpose. To change it, please click this link to turn to [Device Management](#) configuration.

System Up-Time: Provide the time since the BEC 6200WZL is being rebooted.

Current time: Set the current time and date. See the Time Zone section for more information. Click this link to turn to [Time Zone](#) configuration.

Software Version: Software version currently loaded in the router

MAC Address: A unique number that identifies the router

Port Status

Port Status: User can check the status of the port that is router is connecting with, Ethernet, EWAN, 3G (4G) or Wireless

WAN

Port: Name of the WAN connection. Click [Port ▶](#) to enter [WAN Interface](#) configuration page. Click [EWAN ▶](#) (for example) to enter [WAN Profile](#) configuration page.

Operation: Current available operation.

Connection: The current connection status.

IP Address: WAN port IP address.

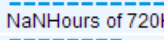

Netmask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

Primary DNS: The IP address of the primary DNS server.

Mobile Status

This section displays the 3G / 4G Card overall status with information such as the current signal strength, statistics of current data transmission and total data transmission.

▼ Mobile Status	
Parameters	
Status	Up
Signal Strength	
SIM Card Status	SIM Card Not Found
Network ID/Name	N/A
Cell ID	01624072(23216242)
Card IMEI	356195050050911
Card IMSI	N/A
Network Mode	WCDMA
Network Band	WCDMA2100
Current TX Bytes / Packets	0 / 0
Current RX Bytes / Packets	0 / 0
Total TX Bytes / Packets	0 / 0
Total RX Bytes / Packets	0 / 0
Mobile usage allowance	
Amount used	 NaNHours of 720Hours
Billing period	 Day:22
<input type="button" value="Refresh"/> <input type="button" value="Clear"/>	

Status: The current status of the 3G/4G-LTE connection.

Signal Strength: The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G-LTE Signal Strength LED indicates the signal strength as well.

SIM Card Status: Display current SIM card status. If it is being installed properly or not.

Signal Information: Shows important LTE signal parameters such as RSRP (Reference Signal Receiving Power), RSRQ (Reference Signal Receiving Quality), SINR (Signal to Interference plus Noise Ratio).

- ▶ RSRP (Reference Signal Receiving Power): is the average power of all resource elements which carry cell-specified reference signals over the entire bandwidth.
- ▶ RSRQ (Reference Signal Receiving Quality): measures the signal strength and is calculated based on both RSRP and RSSI.
- ▶ RSSI (Received Signal Strength Indicator): parameter which provides information about total received wide-band power (measure in all symbols) including all interference and thermal noise. Please refer to the [Hardware/Front LED Indicators](#) for details.
- ▶ SINR (Signal to Interference plus Noise Ratio): is also a measure of signal quality as well. It is widely used by the operators as it provides a clear relationship between RF conditions and throughput. **NOTE: Some LTE modules do not provide this information.**

Network ID/Name: The ID or name of the LTE network the router is connecting to.

Cell ID: The ID of base station that the device is connected to.

Card IMEI: The unique identification number that is used to identify the 3G/4G-LTE module.

Card IMSI: The international mobile subscriber identity used to uniquely identify the 3G/4G-LTE module.

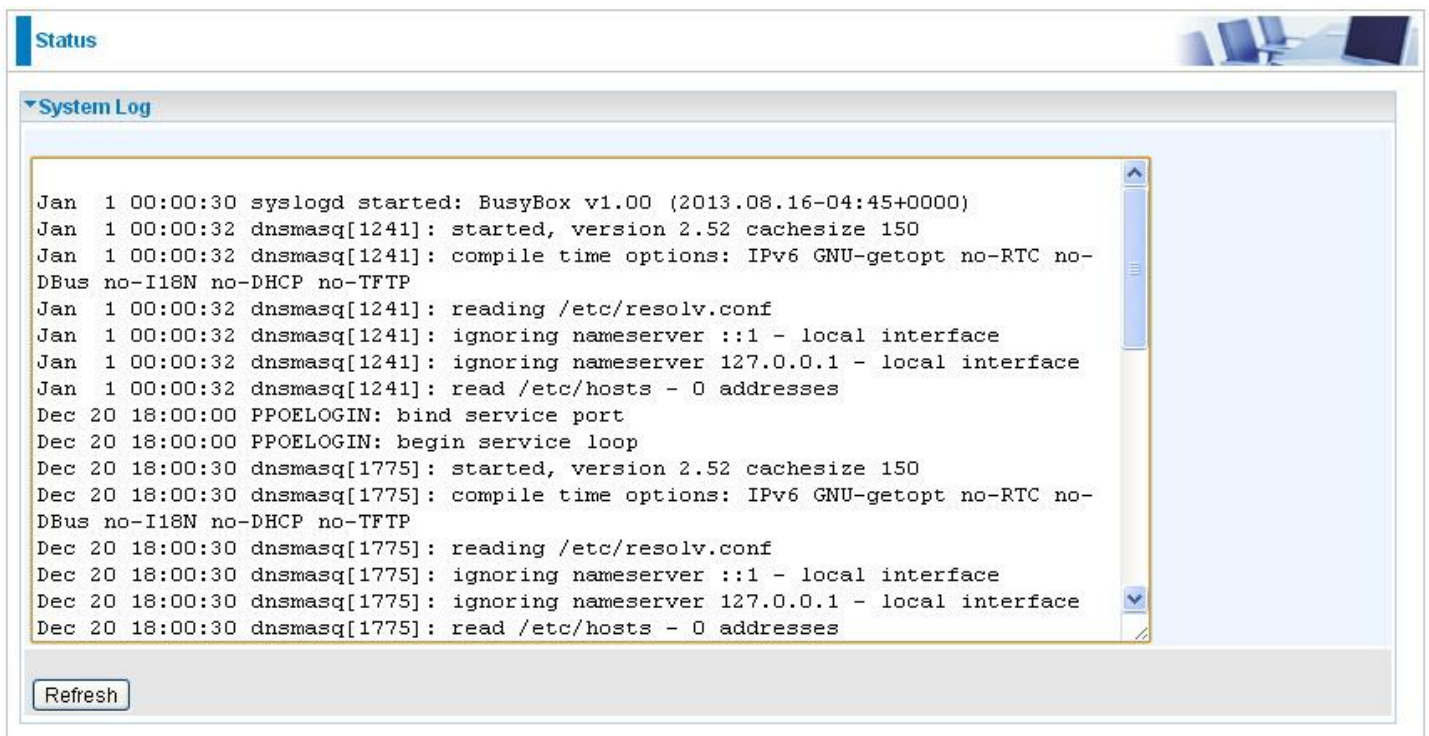
Network Mode: Show the using network mode.

Network Band: Show the using network band.

Refresh: Press this button to refresh the statistics.

System Log

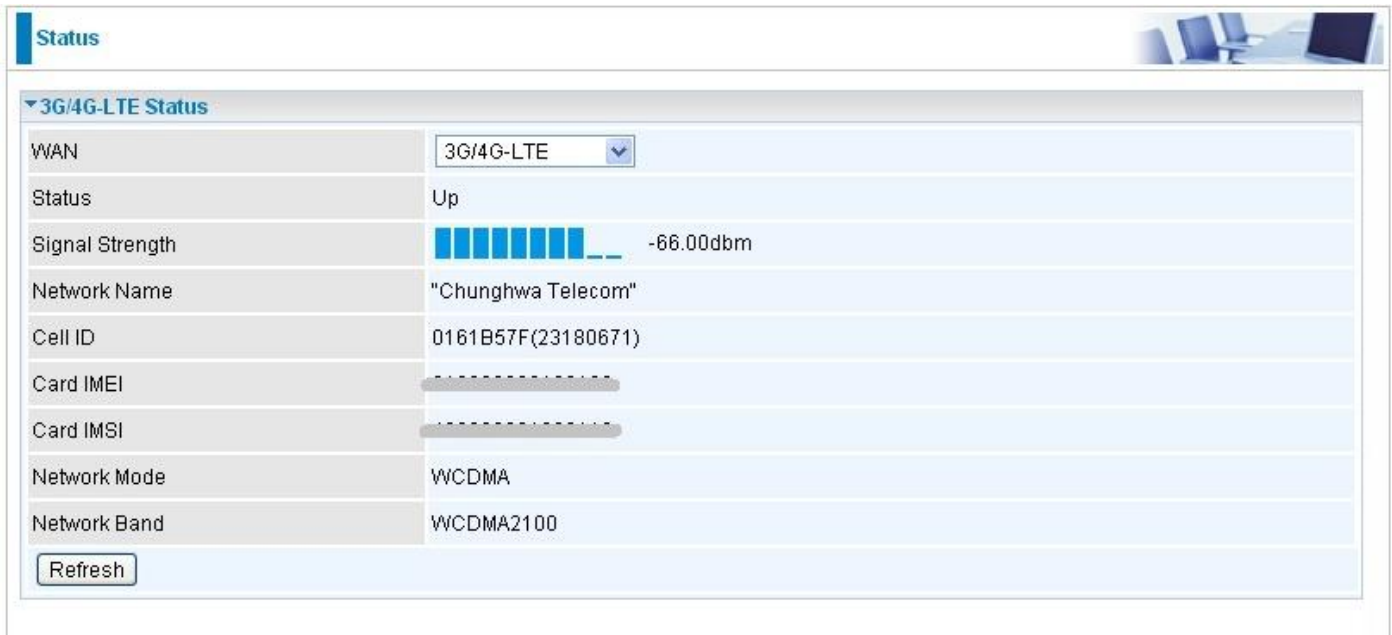
In system log, you can check the operations status and any glitches to the router.



Refresh: Press this button to refresh the statistics.

3G/4G-LTE Status

This page contains 3G/4G-LTE connection information.



The screenshot shows a web interface for 'Status' with a '3G/4G-LTE Status' section. It displays various connection parameters in a table-like format. A 'Refresh' button is located at the bottom of the section.

3G/4G-LTE Status	
WAN	3G/4G-LTE
Status	Up
Signal Strength	<div><div></div></div> -66.00dbm
Network Name	"Chunghwa Telecom"
Cell ID	0161B57F(23180671)
Card IMEI	
Card IMSI	
Network Mode	WCDMA
Network Band	WCDMA2100

Refresh

Status: The current status of the 3G/4G-LTE connection.

Signal Strength: The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G-LTE Signal Strength LED indicates the signal strength as well.

Signal Information: Shows important LTE signal parameters such as RSRP (Reference Signal Receiving Power), RSRQ (Reference Signal Receiving Quality), SINR (Signal to Interference plus Noise Ratio).

- ▶ **RSRP (Reference Signal Receiving Power):** is the average power of all resource elements which carry cell-specified reference signals over the entire bandwidth.
- ▶ **RSRQ (Reference Signal Receiving Quality):** measures the signal strength and is calculated based on both RSRP and RSSI.
- ▶ **RSSI (Received Signal Strength Indicator):** parameter which provides information about total received wide-band power (measure in all symbols) including all interference and thermal noise. Please refer to the [Hardware/Front LED Indicators](#) for details.
- ▶ **SINR (Signal to Interference plus Noise Ratio):** is also a measure of signal quality as well. It is widely used by the operators as it provides a clear relationship between RF conditions and throughput. **NOTE: Some LTE modules do not provide this information.**

Network Name: The name of the LTE network the router is connecting to.

Cell ID: The ID of base station that the device is connected to.

Card IMEI: The unique identification number that is used to identify the 3G/4G-LTE module.

Card IMSI: The international mobile subscriber identity used to uniquely identify the 3G/4G-LTE module.

Network Mode: Show the using network mode.

Network Band: Show the using network band.

Total TX Bytes / Packets: The statistics of total data transmission in bytes / packets since system ready.

Total RX Bytes / Packets: The statistics of total data received in bytes / packets since system ready.

Amount used: Show the traffic or hours has been used.

Billing period: The day from which the fee is charged.

Refresh: Press this button to refresh the statistics.

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall - MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.

Status			
▼ ARP Table			
Wired & Wireless			
IP Address	MAC Address	Interface	Static ARP
192.168.1.100	18:A9:05:38:04:03	lan	No
172.16.1.254	00:50:7F:E0:B1:14	wan	No

IP Address: It is IP Address of internal host that join this network.

MAC Address: The MAC address of internal host.

Interface: indicates which side the IP addresses locate on. WAN means the corresponding IP locates on WAN side.

Static ARP: The state for ARP.

- ▶ **“No”** for dynamically-generated ARP table entries.
- ▶ **“Yes”** for static ARP table entries added by the user.

DHCP Table

Status			
▼ DHCP Table			
Leased Table			
IP Address ▶	MAC Address	Client Host Name	Register Information
192.168.1.100	18:a9:05:38:04:03	billion-17bc6f1	Remains11:30:11

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

Client Host Name: Show the hostname of the PC.

Register Information: Register time information.

System Log

Display system logs accumulated up to the present time. You can trace historical information with this function.

Status

▼ System Log

Current Time: Wed Aug 15 22:14:09 2012

Aug 15 22:13:07 PPPoE: Using interface ppp255
Aug 15 22:13:07 PPPoE: Connection start.
Aug 15 22:13:10 PPPoE: add ci req netmask 1
Aug 15 22:13:10 PPPoE: add ci netmask 0.0.0.0
Aug 15 22:13:10 PPPoE: LCP terminated by peer
Aug 15 22:13:13 PPPoE: Connection terminated.
Aug 15 22:13:13 PPPoE: Doing disconnect
Aug 15 22:13:43 PPPoE: current devfd = 11
Aug 15 22:13:43 PPPoE: current fd_ppp = 12
Aug 15 22:13:43 PPPoE: Using interface ppp255
Aug 15 22:13:43 PPPoE: Connection start.
Aug 15 22:13:46 PPPoE: add ci req netmask 1
Aug 15 22:13:46 PPPoE: add ci netmask 0.0.0.0
Aug 15 22:13:46 PPPoE: LCP terminated by peer
Aug 15 22:13:46 PPPoE: Connection terminated.

Refresh

Clear

Firewall Log

Firewall Log displays log information of any unexpected action with your firewall settings. This page displays the router's Firewall Log entries. The log shows log entries when you have enabled Intrusion Detection or Block WAN PING in the **Configuration - Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.

Status

▼ Firewall Log

Current Time: Wed Aug 7 00:57:52 2013

Refresh

Clear

BEC 6200WZL User Manual

UPnP Portmap

The section lists all port-mapping established using UPnP (Universal Plug and Play). Please see the Advanced section of this manual for more details on UPnP and the router's UPnP configuration options.

Status				
▼ UPnP Portmap				
Table				
Name	Protocol	External Port	Internal Port	IP Address
Thunder5	TCP	11377	11377	192.168.1.100
Thunder5	UDP	11377	10104	192.168.1.100

Name: the name of this UPnP mapping.

Protocol: the protocol used by this mapping.

External Port: the external service port the internal port mapped to.

Internal Port: the internal service port.

IP Address: the IP Address of the host in LAN.

Quick Start

The Quick Start Wizard is a helpful guide for the first-time users to the device and will guide you step by step to setup your BEC 6200WZL device.

Step 1 – Time Zone

Choose your time zone. Click **NEXT** to continue.

The screenshot shows the 'Quick Start' wizard interface. Under the 'Time Zone' section, there are two radio buttons: 'Enable' (selected) and 'Disable'. Below them is a dropdown menu for 'Local Time Zone (+GMT Time)' with the selected value '(GMT-06:00) Central Time (US & Canada)'. At the bottom of the section is a 'Continue' button.

Step 2 – WAN

Set up your Internet connection.

Select an appropriate WAN connection mode then click **Continue** to the next step.

To skip the WAN setting, click "**Jump to Wireless Setting**" to setup local wireless network.

The screenshot shows the 'Quick Start' wizard interface for the 'WAN Port' section. It has a breadcrumb 'WAN > Wireless'. The 'Select WAN Port' section contains a 'Connect Mode' dropdown set to 'EWAN (Recommended)' and a 'Protocol' dropdown set to 'Obtain an IP Address Automatically'. At the bottom are 'Continue' and 'Jump to Wireless setting' buttons.

2.1 If selected **EWAN / Obtain an IP Address Automatically**

Simply click on the **Apply** button to continue to the next step.

The screenshot shows the 'Configuration' screen for the 'WAN Port' section. It has a breadcrumb 'WAN Port'. Under 'WAN Connection', the 'Main Port' dropdown is set to 'EWAN' with a note '(Current Main Port : EWAN)'. Under 'Parameters', the 'Protocol' dropdown is set to 'Obtain an IP Address Automatically'. At the bottom are 'Apply' and 'Cancel' buttons.

2.2 If selected **EWAN / Fixed IP Address** (for example).

Please manually enter the assigned WAN IP information provided by your ISP. Click on Apply to continue.

Configuration

▼ WAN Port

WAN Connection

Main Port EWAN (Current Main Port : EWAN)

Parameters

Protocol Fixed IP Address

IP Address

Netmask

Gateway

2.3 If selected **EWAN / PPPoE**

Please enter PPPoE account information provided by your ISP. Click on Apply to continue

Configuration

▼ WAN Port

WAN Connection

Main Port EWAN (Current Main Port : EWAN)

Parameters

Protocol PPPoE

Username

Password

Service Name

IP Address ('0.0.0.0' means 'Obtain an IP address automatically')

Authentication Protocol Auto

2.4 If selected **3G/4G-LTE**

Input all relevant 3G/4G-LTE parameters from your ISP.

Quick Start

▼ WAN Port

WAN Connection

Main Port 3G/4G (Current Main Port : 3G)

Parameters

ISP Mode AT&T_US

TEL No.

APN

Username

Password

Authentication Protocol Auto

PIN

*Warning: Entering the wrong PIN code three times will lock the SIM.

Note: when re-inserting the 3G / 4G SIM card to the BEC 6200WZL, you should again press **Apply** button to make 3G / 4G connection take effort, or you can Save Config and Restart the router to reach the same effort.

Step 3 – Wireless

Set up your wireless connection if you want to connect to the Internet wirelessly on your PCs. Click on Continue to the next step

Quick Start

▼ Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
Channel ID	Auto
Security Mode	WPA/WPA2 Pre-Shared Key
Regulation Domain	N.America
WPA Shared Key	0004ED012340

Continue

Step 4 – Saving Configuration

Quick Start

▼ Save configuration

Saving configuration to FLASH. Please wait for 10 seconds

Step 5 – Quick Start Completed!

You now may be able to access to the Internet. If not, please check your WAN, Internet Connection, setup again.

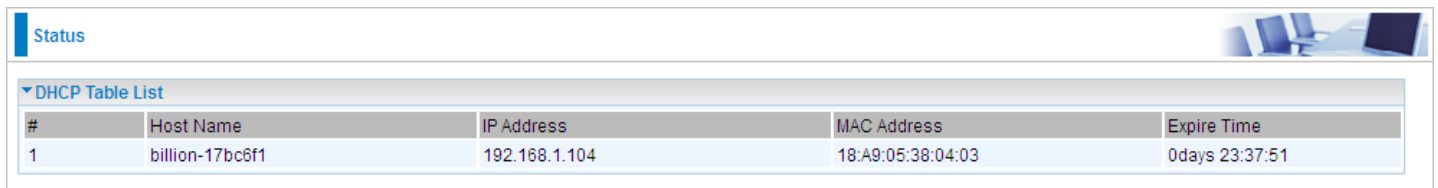
Quick Start

▼ Process finished

Success.

The Quick Start process is finished. Your device has been successfully configured.

DHCP table displays the devices connected to the router with clear information.



The screenshot shows a web-based configuration interface. At the top left is a 'Status' tab. Below it is a section titled 'DHCP Table List' with a dropdown arrow. This section contains a table with five columns: '#', 'Host Name', 'IP Address', 'MAC Address', and 'Expire Time'. There is one data row with the following values: '# 1', 'Host Name billion-17bc6f1', 'IP Address 192.168.1.104', 'MAC Address 18:A9:05:38:04:03', and 'Expire Time 0days 23:37:51'. In the top right corner of the interface, there is a small icon depicting a desk with a laptop and two chairs.

#	Host Name	IP Address	MAC Address	Expire Time
1	billion-17bc6f1	192.168.1.104	18:A9:05:38:04:03	0days 23:37:51

#: The index identifying the connected devices.

Host Name: Show the hostname of the PC.

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

Expire Time: The total remaining interval since the IP assignment to the PC.

Configuration

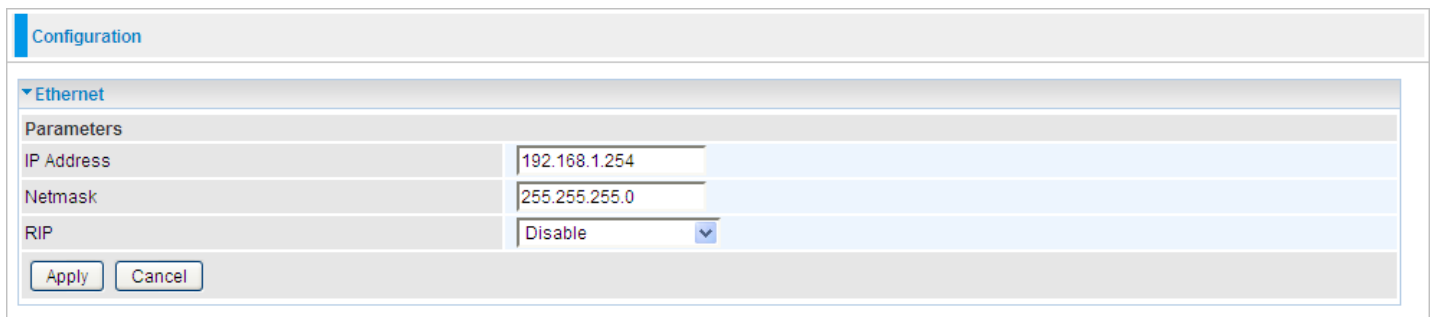
Click to access and configure the available features in the following: **LAN, WAN, System, Firewall, QoS, Virtual Server, Wake on LAN, Time Schedule, and Advanced.**

These functions are described in the following sections.

LAN (Local Area Network)

Here are the features under **Interface Setup: Ethernet, IP Alias, Wireless, Wireless Security, WPS, and DHCP Server.**

Ethernet



Configuration

▼ Ethernet

Parameters

IP Address 192.168.1.254

Netmask 255.255.255.0

RIP Disable

Apply Cancel

The router supports more than one Ethernet IP addresses in the LAN, and with distinct LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.

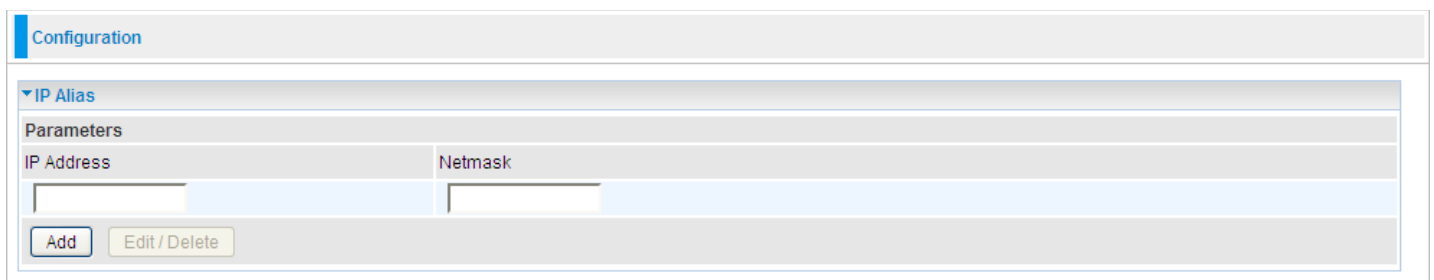
IP Address: The IP on this router, default is 192.168.1.254.

Netmask: The subnet mask on this router.

RIP: RIP v1, RIP v2 Broadcast, RIP v1+v2 Broadcast and RIP v2 Multicast.

IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.



Configuration

▼ IP Alias

Parameters


IP Address Netmask

Add Edit / Delete

IP Address: Specify an IP address on this virtual interface.

Netmask: Specify a subnet mask on this virtual interface.

Wireless

Configuration


Wireless

Parameters

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	Wireless G+N
Number of Active SSID	1
SSID No.	SSID1
ESSID	wlan-ap
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20/40MHZ
Tx PowerLevel	100 (0 ~ 100)
AP MAC Address	00:1D:92:C0:13:CD
AP Firmware Version	2.3.0.0
WPS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WPS State	<input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

** WDS depends on the settings of main security encryption type. **

Apply Cancel Security settings

Wireless Parameters

WLAN Service: Default setting is set to **Enable**.

Mode: The default setting is **Wireless G + N** (Mixed mode). If you do not know or have both 11g and 11n devices in your network, then keep the default in **mixed mode**. From the drop-down manual, you can select **Wireless – G** if you have only 11g card. If you have only 11b card, then select **Wireless – B**. If you have only 11n card, then select **Wireless – N**.

Number of Active SSID: Number of SSID you can choose.

SSID No.: The SSID you choose.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Note: ESSID is case sensitive and must not excess 32 characters.

Hide ESSID: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Disable**.

- **Enable:** Select Enable if you do not want broadcast your ESSID. When select Enable, the ESSID will be hidden instead of broadcasting, thus when wireless client searches for this AP, failure occurs. This ESSID(AP) will be invisible to you. In this case, if you want to join this wireless network, enter the exactly ESSID manually and some security settings.
- **Disable:** When Disable is selected, the router will broadcast the ESSID to allow anybody with a wireless client to be able to identify the Access Point (AP) of your router. Select the specific

ESSID scanned, with some security settings, you will join this wireless network.

Regulation Domain: There are seven Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

Channel ID: Select the ID channel that you would like to use.

Channel Width: Select either **20 MHz** or **20/40 MHz** for the channel bandwidth. The higher the bandwidth the better the performance will be.

Tx Power Level: It is function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 0 up to maximum 100.

Note: The Power Level maybe different in each access network user premises environment and choose the most suitable level for your network.

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

WPS service: Enable / disable

WPS State: Current WPS state in AP. It is be used for WCN (Windows Connect Now).

- ▶ **Configured:** This AP is be configured via WPS and not allow to be configured via WCN.
- ▶ **Unconfigured:** This AP is un-configured via WPS. It can be configure via WCN.

WMM: This feature works concurrently with QoS that enables the system to prioritize the flow of data packets according to 4 categories: Voice, Video, Best Efforts and Background.

- ▶ **Enable:** Click to activate WMM feature.
- ▶ **Disable:** Click to deactivate WMM feature.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed, simply define the peer's MAC address of the connected AP. WDS takes advantages of cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

WDS Service: The default setting is **Disable**. Check **Enable** radio button to activate this function.

1. **Peer WDS MAC Address:** It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.
2. **Peer WDS MAC Address:** It is the second associated AP's MAC Address.
3. **Peer WDS MAC Address:** It is the third associated AP's MAC Address.
4. **Peer WDS MAC Address:** It is the fourth associated AP's MAC Address.

Note: For MAC Address, Semicolon (;) or Dash (-) must be included.

Wireless Security

You can disable or enable with WPA or WEP for protecting wireless network.

The screenshot shows the 'Configuration' tab with the 'Wireless Security' section expanded. Under 'Parameters', the following settings are visible: SSID No. is set to 'ESSID1'; Security Mode is set to 'WPA/WPA2 Pre-Shared Key'; WPA Algorithms is set to 'AES'; WPA Shared Key is '0004ED012340'; and Group Key Renewal is '3600' seconds. 'Apply' and 'Cancel' buttons are at the bottom.

Parameters	
SSID No.	ESSID1
Security Mode	WPA/WPA2 Pre-Shared Key
WPA Algorithms	AES
WPA Shared Key	0004ED012340
Group Key Renewal	3600 seconds

SSID No.: Choose the SSID you want to set.

Security Mode: There are five security modes for you to choose.

► WPA Pre-Shared Key

This screenshot is similar to the previous one but shows the 'Security Mode' set to 'WPA Pre-Shared Key' instead of 'WPA/WPA2 Pre-Shared Key'. All other parameters remain the same.

Parameters	
SSID No.	ESSID1
Security Mode	WPA Pre-Shared Key
WPA Algorithms	AES
WPA Shared Key	0004ED012340
Group Key Renewal	3600 seconds

WPA Algorithms: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

► **WPA2 Pre-Shared Key**

The screenshot shows a web-based configuration page for a network device. At the top, there is a 'Configuration' tab. Below it, a 'Wireless Security' section is expanded, showing a 'Parameters' table. The table has the following fields: 'SSID No.' with a dropdown menu showing 'ESSID1'; 'Security Mode' with a dropdown menu showing 'WPA2 Pre-Shared Key'; 'WPA Algorithms' with a dropdown menu showing 'AES'; 'WPA Shared Key' with a text input field containing '0004ED012340'; and 'Group Key Renewal' with a text input field containing '3600' and a unit label 'seconds'. At the bottom of the table, there are 'Apply' and 'Cancel' buttons.

Parameters	
SSID No.	ESSID1
Security Mode	WPA2 Pre-Shared Key
WPA Algorithms	AES
WPA Shared Key	0004ED012340
Group Key Renewal	3600 seconds

Apply Cancel

WPA Algorithms: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

► **WPA / WPA2 Pre-Shared Key**

The screenshot shows a web-based configuration page for a network device. At the top, there is a 'Configuration' tab. Below it, a 'Wireless Security' section is expanded, showing a 'Parameters' table. The table has the following fields: 'SSID No.' with a dropdown menu showing 'ESSID1'; 'Security Mode' with a dropdown menu showing 'WPA/WPA2 Pre-Shared Key'; 'WPA Algorithms' with a dropdown menu showing 'AES'; 'WPA Shared Key' with a text input field containing '0004ED012340'; and 'Group Key Renewal' with a text input field containing '3600' and a unit label 'seconds'. At the bottom of the table, there are 'Apply' and 'Cancel' buttons.

Parameters	
SSID No.	ESSID1
Security Mode	WPA/WPA2 Pre-Shared Key
WPA Algorithms	AES
WPA Shared Key	0004ED012340
Group Key Renewal	3600 seconds

Apply Cancel

WPA Algorithms: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

► WEP

Configuration

▼ Wireless Security

Parameters

SSID No.	ESSID1	
Security Mode	WEP	
WEP Authentication	Open System	
Default Used WEP Key	<input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	
Passphrase (Generate Key)	<input type="text"/> <input type="button" value="WEP64"/> <input type="button" value="WEP128"/>	
Key 1	Hex	<input type="text"/>
Key 2	Hex	<input type="text"/>
Key 3	Hex	<input type="text"/>
Key 4	Hex	<input type="text"/>

WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX. 11aa22cc33.
 WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
 WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX. 11aa22cc33dd44ee55efffe35f.
 WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?!dbd3ert.

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are three options to select from: **Open System**, **Share key** or **Both**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the **Passphrase** is enabled.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively-no any separator is included.

WPS

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN (Personal Information Number) Method** & **PBC (Push Button Configuration) Method**.

Configuration

▼ WPS

Parameters

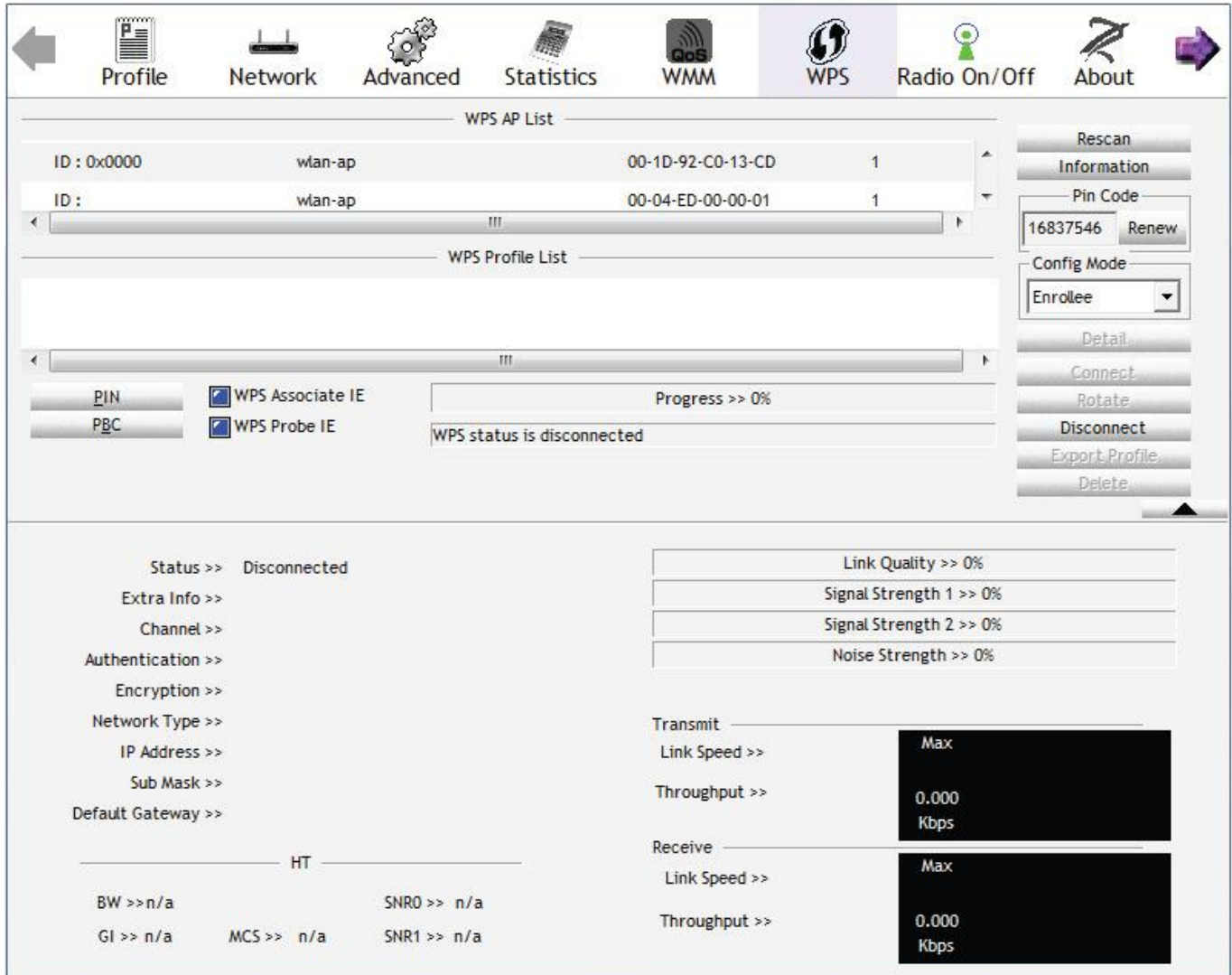
WPS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Role	<input checked="" type="radio"/> Registrar <input type="radio"/> Enrollee
WPS PIN	25879810
Enrollee's PIN	<input type="text"/>

Wi-Fi Protected Setup (WPS) Example I:

PIN Method (Personal Information Number): Configure AP as Registrar

Use Ralink Wireless Utility for example.

1. Write down the PIN code (e.g. 16837546) from a WPS utility (e.g. Ralink Utility)



2. In the BEC 6200WZL, please enter the Enrollee (Client) PIN code (e.g. 16837546) from Ralink Utility and then press **Start**.

Configuration

WPS

Parameters

WPS Service

☒ Enable
 ☐ Disable

Role

☒ Registrar
 ☐ Enrollee

WPS PIN

25879810

Enrollee's PIN

16837546

Start

Cancel

3. Now, go back to the Ralink Utility

- Change the Config Mode to Enrollee
- Press the WPS button on the top bar again to flash the utility
- Find the SSID of your BEC 6200WZL (e.g. Billion_AP) from the WPS AP List column.
- Press the **PIN** button to run the scan and connect with BEC 6200WZL.

Profile

Network

Advanced

Statistics

WMM

WPS

Radio On/Off

About

WPS AP List

ID :	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1

WPS Profile List

wlan-ap

PIN

PBC

☒ WPS Associate IE
 ☒ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

Rescan

Information

Pin Code

16837546 Renew

Config Mode

Enrollee

Detail

Connect

Rotate

Disconnect

Export Profile

Delete

Status >> wlan-ap <--> 00-1D-92-C0-13-CD

Extra Info >> Link is Up [TxPower:100%]

Channel >> 1 <--> 2412 MHz; central channel : 3

Authentication >> Open

Encryption >> NONE

Network Type >> Infrastructure

IP Address >> 192.168.1.100

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.1.254

HT

BW >> 40

SNR0 >> 19

GI >> long

MCS >> 15

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 64%

Signal Strength 2 >> 34%

Noise Strength >> 26%

Transmit

Link Speed >> 270.0 Mbps

Throughput >> 5.600 Kbps

Max

38.624 Kbps

Receive

Link Speed >> 54.0 Mbps

Throughput >> 81.608 Kbps

Max

146.840 Kbps

Wi-Fi Protected Setup (WPS) Example II:

PIN Method (Personal Information Number): Configure AP as Enrollee

Use Ralink Wireless Utility for example.

1. Launch to BEC 6200WZL GUI, go to the WPS configuration section to change WPS Role to **Enrollee** then press the **Start** button for activation.
2. Write down the WPS PIN (e.g. 25879810) from the BEC 6200WZL.

Configuration	
▼ WPS	
Parameters	
WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Role	<input type="radio"/> Registrar <input checked="" type="radio"/> Enrollee
WPS PIN	25879810
Mode	PIN
<input type="button" value="Start"/> <input type="button" value="Cancel"/>	

3. Now, go back to the Ralink Utility

- Change the Config Mode to Registrar
- In the PIN code box, enter the WPS PIN from BEC 6200WZL (e.g. 25879810)
- Find the SSID of your BEC 6200WZL (e.g. Billion_AP) from the WPS AP List column.
- Press the **PIN** button to run the scan and connect with BEC 6200WZL

If successful, the BEC 6200WZL Wireless SSID and the security setting will be identical with the Ralink Wireless Utility.

←

Profile

Network

Advanced

Statistics

WMM

WPS

Radio On/Off

About

→

WPS AP List

ID :	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-22-22-23	1

WPS Profile List

ExRegNWEA4036

PIN

PBC

☒ WPS Associate IE

Progress >> 0%

☒ WPS Probe IE

WPS status is disconnected

Rescan

Information

Pin Code

25879810

Renew

Config Mode

Registrar

Detail

Connect

Rotate

Disconnect

Export Profile

SSID >>

ExRegNWEA4036

BSSID >>

00-00-00-00-00-00

Authentication Type >>

WPA2-PSK

Encryption Type >>

AES

Key Length >>

5

Key Index >>

1

Key Material >>

811B5B9F3403DCB08BA73BF3E4787581C37DC4BDD147C4E62526D4E8C39DBF78

☒ Show Password

OK

Cancel

Configuration

Wireless Security

Parameters

SSID No.	ESSID1	
Security Mode	WPA2 Pre-Shared Key	
WPA Algorithms	AES	
WPA Shared Key	811B5B9F3403DCB08I	
Group Key Renewal	3600	seconds

Apply

Cancel

Wi-Fi Protected Setup (WPS) Example III:

PIN Method (Personal Information Number): Configure AP as Enrollee

Use Window Vista WCN (Windows Connect Now) for WPS setup

1. Launch to BEC 6200WZL GUI, go to WPS section then write down the WPS PIN (e.g. 25879810)

WPS Parameters	
WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Role	<input type="radio"/> Registrar <input checked="" type="radio"/> Enrollee
WPS PIN	25879810
Mode	PIN

Start Cancel

2. Go to Wireless section in the GUI

- Enable **WPS Service**
- Next to **WPS State**, enable **Unconfigured**
- Then click “Apply” to save settings.

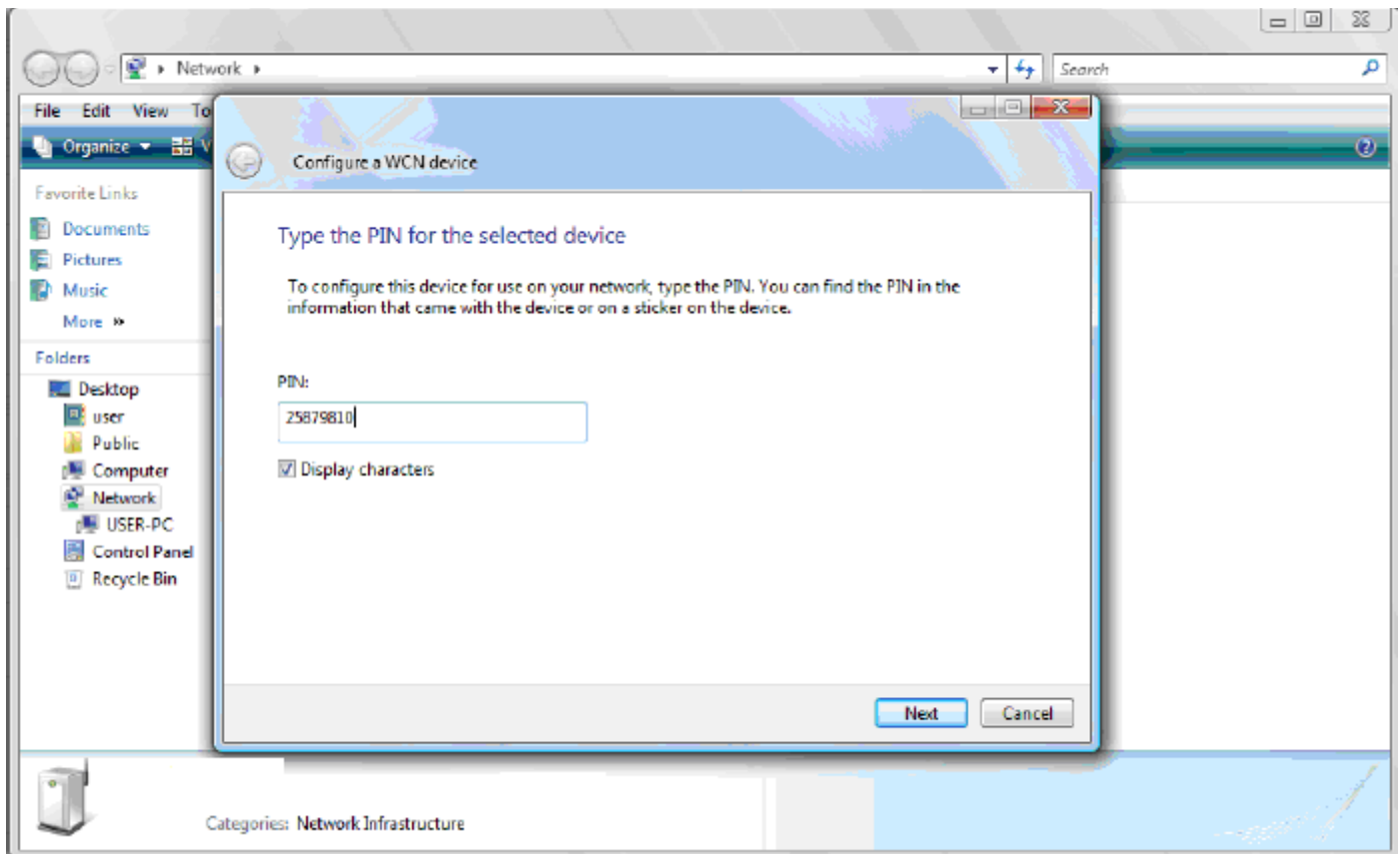
Advanced Configuration	
SSID No.	<input checked="" type="radio"/> SSID1
ESSID	wlan-ap
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20MHZ
Tx PowerLevel	100 (0 ~ 100)
AP MAC Address	00:04:ED:35:52:62
AP Firmware Version	2.3.0.0
WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WPS State	<input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

** WDS depends on the settings of main security encryption type. **

Apply Cancel Security settings

3. Now, go to your PC or Notebook

- Open the **Control Panel**, go to **Network and Internet** then **View Network Computers and Devices**. Double click on router icon then enter the WPS PIN number from BEC 6200WZL (e.g. 25879810)




- Enter the Wireless SSID of your BEC 6200WZL (e.g. Billion_AP)
- Enter a Passphrase.

If successful, your PC / Notebook should now be connected with the BEC 6200WZL.

Wi-Fi Protected Setup (WPS) Example IV:

PBC (Push Button Configuration) Method:

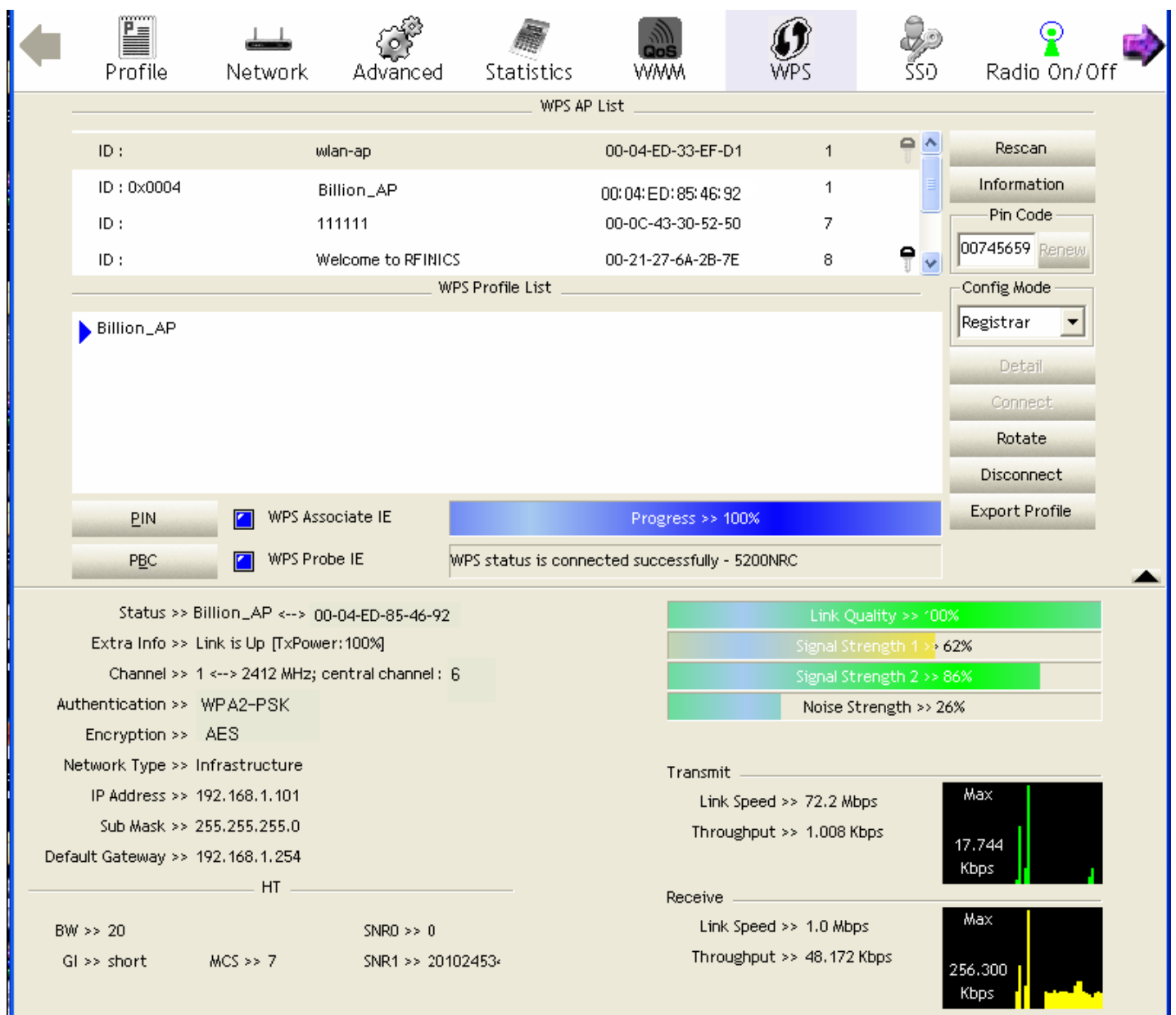
Example is based on Ralink Wireless Utility

1. On the back of the BEC 6200WZL, press and hold the WPS hardware button () for 2-3 seconds then release.

2. Now, go to the Ralink Utility

- Change the Config Mode to Enrollee
- Find the SSID of your BEC 6200WZL (e.g. Billion_AP) from the WPS AP List column.
- Press the **PBC** button to run the scan and connect with BEC 6200WZL

If successful, the BEC 6200WZL Wireless SSID and the security setting will be identical with the Ralink Wireless Utility.



WPS AP List

ID :	SSID	MAC	Channel
wlan-ap		00-04-ED-33-EF-D1	1
ID : 0x0004	Billion_AP	00:04:ED:85:46:92	1
ID :	111111	00-0C-43-30-52-50	7
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8

WPS Profile List

Billion_AP

Config Mode: Registrar

Buttons: Rescan, Information, Pin Code (00745659), Renew, Detail, Connect, Rotate, Disconnect, Export Profile

PIN: WPS Associate IE: ☒ Progress >> 100%

PBC: ☒ WPS Probe IE: ☒ WPS status is connected successfully - 5200NRC

Status >> Billion_AP <--> 00-04-ED-85-46-92

Extra Info >> Link is Up [TxPower:100%]

Channel >> 1 <--> 2412 MHz; central channel : 6

Authentication >> WPA2-PSK

Encryption >> AES

Network Type >> Infrastructure

IP Address >> 192.168.1.101

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.1.254

HT

BW >> 20 SNR0 >> 0

GI >> short MCS >> 7 SNR1 >> 20102453

Link Quality >> 100%

Signal Strength 1 >> 62%

Signal Strength 2 >> 86%

Noise Strength >> 26%

Transmit

Link Speed >> 72.2 Mbps

Throughput >> 1,008 Kbps

Max 17,744 Kbps

Receive

Link Speed >> 1.0 Mbps

Throughput >> 48,172 Kbps

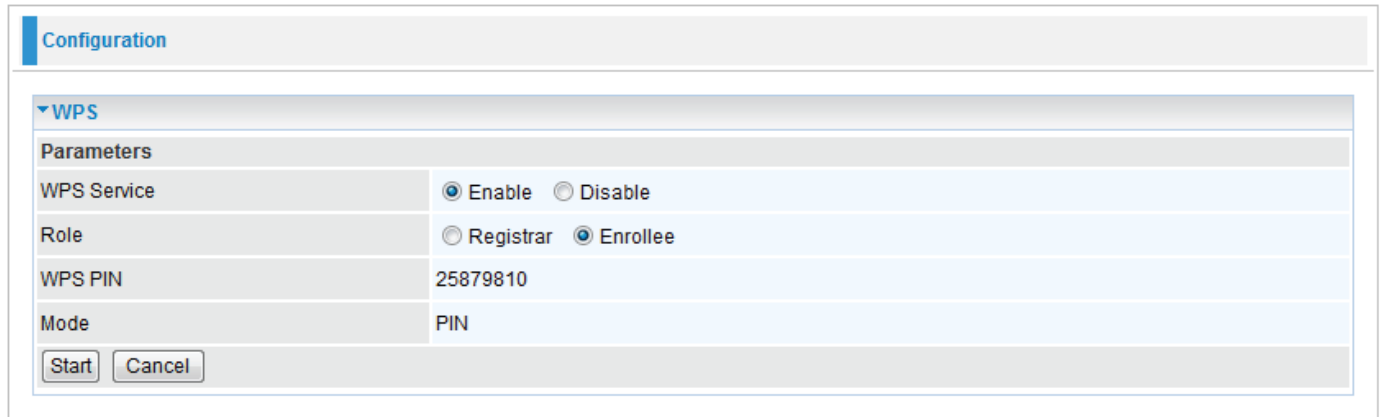
Max 256,300 Kbps

Wi-Fi Protected Setup (WPS) Example V:

PBC (Push Button Configuration) Method:

Example is based on Ralink Wireless Utility

2. Write down the WPS PIN (e.g. 25879810) from the BEC 6200WZL.



The screenshot shows the 'Configuration' window of the Ralink Wireless Utility. The 'WPS' section is expanded, showing the following parameters:

Parameters	
WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Role	<input type="radio"/> Registrar <input checked="" type="radio"/> Enrollee
WPS PIN	25879810
Mode	PIN

At the bottom of the WPS section, there are two buttons: 'Start' and 'Cancel'.

3. Now, go back to the Ralink Utility

- Change the Config Mode to Registrar
- In the PIN code box, enter the WPS PIN from BEC 6200WZL (e.g. 25879810)
- Find the SSID of your BEC 6200WZL (e.g. Billion_AP) from the WPS AP List column.
- Press the **PIN** button to run the scan and connect with BEC 6200WZL

If successful, the BEC 6200WZL Wireless SSID and the security setting will be identical with the Ralink Wireless Utility.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

DHCP Server Mode: Disable

To disable the router's DHCP Server, check **Disabled** and then click **Apply**. When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (the default is 192.168.1.254).

The screenshot shows the 'Configuration' tab of a router's web interface. Under the 'DHCP Server' section, the 'Parameters' table has 'DHCP Server Mode' set to 'Disable' in a dropdown menu. An 'Apply' button is visible below the table. At the bottom, a status bar indicates 'Current Mode: DHCP Server'.

Parameters	
DHCP Server Mode	Disable

Apply

Current Mode: DHCP Server

DHCP Server Mode: DHCP Server

To configure the router's DHCP Server, check **DHCP Server**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the 3G / 4G Router performs the domain name lookup, finds the IP address from the outside network automatically and forwards it back to the requesting PC in the LAN (your Local Area Network).

The screenshot shows the 'Configuration' tab of a router's web interface. Under the 'DHCP Server' section, the 'Parameters' table has 'DHCP Server Mode' set to 'DHCP Server'. Other parameters are filled in: 'Domain Name' is 'home.gateway', 'Range Start' is '192.168.1.100', 'Range End' is '192.168.1.199', 'Default Lease Time' is '43200' seconds, and 'Maximum Lease Time' is '86400' seconds. The 'Use Router as DNS Server' checkbox is checked. 'Primary DNS Server Address' and 'Secondary DNS Server Address' are empty. An 'Apply' button and a 'Fixed Host' link are at the bottom. The status bar shows 'Current Mode: DHCP Server'.

Parameters	
DHCP Server Mode	DHCP Server
Domain Name	home.gateway
Range Start	192.168.1.100
Range End	192.168.1.199
Default Lease Time	43200 seconds
Maximum Lease Time	86400 seconds
Use Router as DNS Server	<input checked="" type="checkbox"/>
Primary DNS Server Address	
Secondary DNS Server Address	

Apply Fixed Host

Current Mode: DHCP Server

DHCP option 66: This option is used to identify a TFTP server for convenient configuration downloading for clients. **Enable** to use option 66 and enter the TFTP server IP or domain name.

Configuration

▼ DHCP Server

Parameters

DHCP Server Mode	DHCP Server ▼	
Domain Name	home.gateway	
Range Start	192.168.1.100	
Range End	192.168.1.199	
Default Lease Time	43200	seconds
Maximum Lease Time	86400	seconds
Use Router as DNS Server	<input checked="" type="checkbox"/>	
Option 66	<input type="checkbox"/> Enable	
Primary DNS Server Address		
Secondary DNS Server Address		

Current Mode: DHCP Server

DHCP Server Mode: DHCP Relay

If you check **DHCP Relay** and then you must enter the IP address of the DHCP server which assigns an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click **Apply** to enable this function.

Configuration

▼ DHCP Server

Parameters

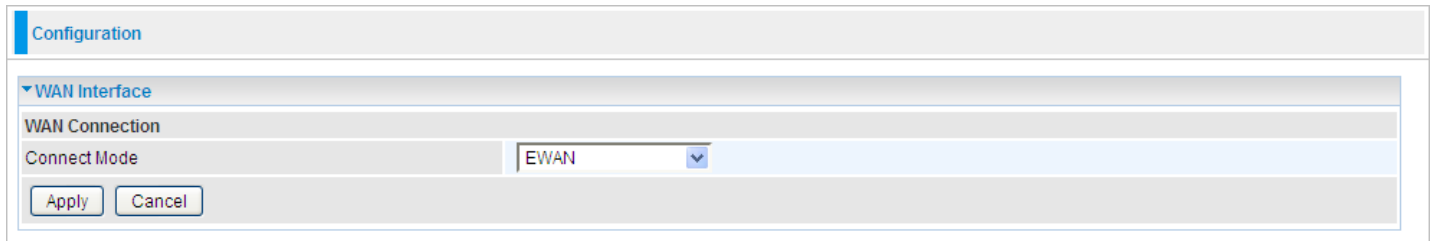
DHCP Server Mode	DHCP Relay ▼	
DHCP Relay Server		

Current Mode: DHCP Server

WAN (Wide Area Network)

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are two items within the **WAN** section: **WAN interface** and **WAN Profile**.

WAN Interface (EWAN)



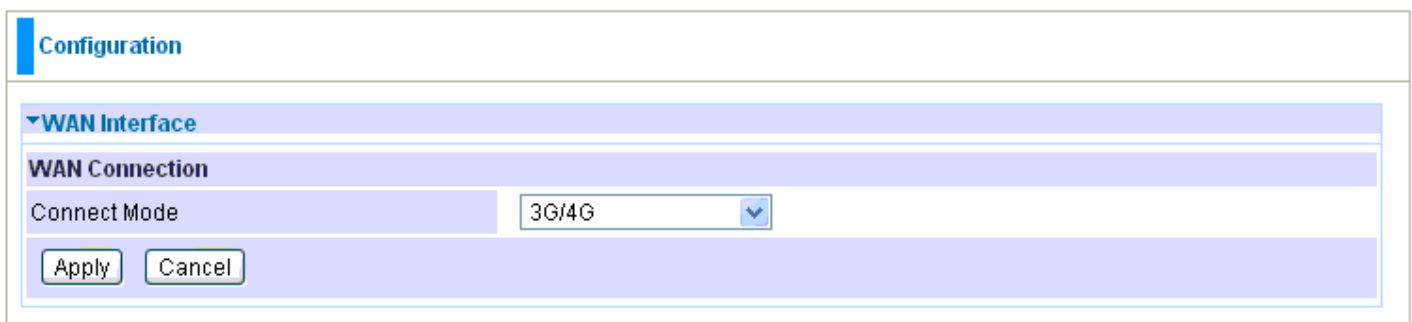
The screenshot shows the 'Configuration' tab of a network device. Under the 'WAN Interface' section, the 'WAN Connection' is set to 'EWAN'. The 'Connect Mode' dropdown menu is also set to 'EWAN'. There are 'Apply' and 'Cancel' buttons at the bottom of the configuration area.

Connect Mode: Select **EWAN** from the drop-down menu.

Click **Apply** to confirm the change.

Go to **WAN Profile** to setup your WAN connection.

WAN Interface (3G / 4G)



The screenshot shows the 'Configuration' tab of a network device. Under the 'WAN Interface' section, the 'WAN Connection' is set to '3G/4G'. The 'Connect Mode' dropdown menu is also set to '3G/4G'. There are 'Apply' and 'Cancel' buttons at the bottom of the configuration area.

Connect Mode: Select **3G/4G** from the drop-down menu.

Click **Apply** to confirm the change.

Go to **WAN Profile** to setup your WAN connection.

WAN Interface(Dual WAN)

The screenshot shows the 'Configuration' tab for the WAN Interface. Under the 'WAN Connection' section, the 'Connect Mode' is set to 'Dual WAN(Failover)'. The 'Failover Parameters' section includes: 'Main WAN' set to '3G/4G' with a link to '3G/4G'; 'Backup WAN' set to 'EWAN' with a link to 'EWAN'; 'Probe' checked and set to 'Enable'; 'Connectivity Decision' set to 'Not in service when probing failed after 3 consecutive times'; 'Failover Probe Cycle' set to 'Every 12 seconds'; 'Failback Probe Cycle' set to 'Every 4 seconds'; and 'Detect Rule' with radio buttons for 'Ping Gateway' (selected) and 'Ping Host'.

Connect Mode: Select the **Dual WAN (Failover)** from the drop-down menu.

Main WAN: Choose EWAN or 3G / 4G as main WAN. Click the link to go to WAN Profile page to configure its parameters. Click the link beside it to configure the Main WAN connection. Turn to WAN profile in the following part for help.

Backup WAN: Choose the left as backup WAN. Click the link to go to **WAN Profile** page to configure its parameters. Click the link beside it to configure the backup WAN.

Connectivity Decision: Enter the value for the times when probing failed to switch backup port.

Failover Probe Cycle: Set the time duration for the Failover Probe Cycle to determine when the router will switch to the backup connection (backup port) once the main connection (main port) fails.

Note: The time values entered in Failover Probe Cycle field is set for each probe cycle and decided by Probe Cycle duration multiplied by Connection Decision value (e.g. 60 seconds are multiplied by 12 seconds and 5 consecutive fails).

Failback Probe Cycle: Set the time for the Failback Probe Cycle.

Detect Rule (either one):

- ▶ **Ping Gateway:** It will send ping packet to gateway and wait response from gateway in every "Probe Cycle".
- ▶ **Ping Host:** It will send ping packet to specific host and wait response in every "Probe Cycle". The host must be an IP address.

Click **Apply** to save settings.

This connection mode supports failover feature so that you can keep your WAN connection always on. You should first configure the main and backup WAN connection profile.

WAN Profile

Main Port - EWAN

BEC 6200WZL (3G/4G_LTE Cellular Broadband Router) offers a WAN port to connect to Cable Modems and fiber optic lines. This alternative, yet faster method to connect to the internet will provide users with more flexibility to get online.

❖ Obtain an IP Address Automatically (EWAN)

When connecting to the ISP, **BEC 6200WZL (3G/4G_LTE Cellular Broadband Router)** also functions as a DHCP client. The router can automatically obtain an IP address, Netmask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.

The screenshot shows the 'Configuration' page for the WAN Profile. Under the 'Parameters' section, the 'Profile Port' is set to 'EWAN'. The 'Line Speed' is set to '30000 Kbps / 30000 Kbps (Downstream / Upstream)'. The 'Protocol' dropdown menu is highlighted with a red circle and set to 'Obtain an IP Address Automatically'. Below this, the 'NAT' checkbox is checked and labeled 'Enable'. The 'Obtain DNS' checkbox is checked and labeled 'Automatic', with 'Primary' and 'Secondary' fields for IP addresses. The 'MAC Spoofing' checkbox is unchecked. At the bottom are 'Apply' and 'Cancel' buttons.

Line Speed: Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

❖ **PPPoE (EWAN)**

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.

The screenshot shows the 'Configuration' page for a WAN Profile. The 'WAN Profile' section is expanded, showing 'Parameters'. The 'Protocol' is set to 'PPPoE', which is circled in red. The 'Username' is 'user' and the 'Password' is masked with four dots. Other settings include 'Line Speed' at 30000 Kbps, 'NAT' checked, 'Obtain DNS' checked, 'Connection' checked, 'MAC Spoofing' unchecked, 'Service Name' empty, 'Auth. Protocol' set to 'Auto', 'Primary' and 'Secondary' DNS empty, 'Idle Timeout' at 0 min, and 'MTU' at 1492. 'Apply' and 'Cancel' buttons are at the bottom.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive)

Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is **Auto**. Your ISP advises on using **Chap** or **Pap**.

Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

Connection:

- ▶ **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.
- ▶ **Connect to Demand (un-select Always On):** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

❖ Fixed IP Address (EWAN)

Select this option to set static IP information. You will need to enter in the Connection type, IP address, netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, in four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

The screenshot shows the 'Configuration' page with the 'WAN Profile' section expanded. Under 'Parameters', the 'Protocol' dropdown menu is set to 'Fixed IP Address' and is circled in red. Other visible settings include 'Profile Port' set to 'EWAN', 'Line Speed' set to '30000 Kbps / 30000 Kbps (Downstream / Upstream)', 'NAT' checked 'Enable', 'IP Address' set to '0.0.0.0', 'Obtain DNS' set to 'Automatic', and 'MAC Spoofing' set to 'Enable'. There are input fields for 'Netmask', 'Gateway', 'Primary', and 'Secondary' DNS. 'Apply' and 'Cancel' buttons are at the bottom.

Line Speed: Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

IP Netmask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0. Type the netmask assigned to you by your ISP (if given).

Gateway: You must specify a gateway IP address (supplied by your ISP)

Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

Main Port - 3G / 4G

The router allows you to insert a 3G / 4G SIM card into the built-in SIM slot, enabling you to use a, UMTS, GSM, or LTE Internet connection.

WAN Profile	
Parameters	
Profile Port	3G/4G
IP Pass-Through Mode	<input type="checkbox"/> Enable
Usage Allowance	<input type="checkbox"/> Enable
LTE Antenna Diversity	
IMS Mode	
Network Mode	Automatic
ISP Mode	AT&T_US
TEL No.	*99***1#
Dual APN	Single APN
APN	broadband
Username	
Password	
Authentication Protocol	Auto
PIN	
Connection	<input checked="" type="radio"/> Always On <input type="radio"/> Connect on Demand
Keep Alive	<input type="checkbox"/> Enable Keep Alive IP
Lcp echo Interval	seconds
NAT	<input checked="" type="checkbox"/> Enable
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS / Secondary DNS	/
*Warning: Entering the wrong PIN code three times will lock the SIM.	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

IP Pass-through Mode: When **enabled**, BEC 6200WZL is in bridge mode that it does not obtain a WAN IP address; features such as routing capabilities, NAT, firewall, etc, are being disabled. The client router that is behind the BEC 6200WZL now obtains a WAN IP address. When **disabled**, BEC 6200WZL is in router mode that it handles a WAN IP address and all features become available.

Usage Allowance: When **enabled**, you can control and manage your mobile usage. Please click [here](#) for detailed setup instruction.

LTE Antenna Diversity: When **enabled**, the auxiliary antenna will be activated. With **disabled**, only the primary antenna is receiving and transmitting data.

NOTE: When using Yagi antenna, please **DISABLE** the Antenna Diversity feature for utmost performance.

IMS Mode: (for Mobile Service Provider used only)

Network Mode: If you know the appropriate Network mode you need to connect to, please select it from the list; otherwise, select "Automatic."

ISP Mode: A list of 3G / 4G service providers that is available.

TEL No.: The dial string to make a GPRS / 3G user internetworking call. It may be provided by your mobile service provider.

Dual APN: Our 3G/4G router provides your either Single APN (one WAN IP) or Dual APN (dual WAN IP) to meet users' different demands. Enter corresponding APN(s) from your service providers.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you accesses to the internet i.e. Some 3G / 4G operators use the APN 'internet' for their portal. The default value of APN is "internet".

Username: Enter the username provided by your service provider.

Password: Enter the password provided by your service provider.

Auth. Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which authentication type the server is using (when acting as a client), or the authentication type you want the clients to use when they are connecting to you (when acting as a server). When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authentication. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and a PUK code will be required from your network / service provider to unlock it.

NOTE: If you enter an incorrect PIN code three times (3) in a row, your SIM card will be blocked. In this case, please enter your PUK code (it can be supplied by your service provider) and then re-enter your PIN.

Connection:

- ▶ **Always On:** The router will make UMTS/GPRS call when starting up. Enabling Always On, will give you an option of Keep Alive.
- ▶ **Connect to Demand:** When enabling this feature, the BEC 6200WZL will automatically resume its Internet connection when there is a packet requesting from a local LAN device.

Keep Alive: Click to enable keep alive mechanism. User should set the Keep Alive IP to necessitate the always on connection. The IP is used for ping operation to examine whether the connection is still on.

Lcp echo Interval: Set the interval time (seconds), if set to 5, that means the router is allowed to send message out every 5sec to prevent the connection being dropped by ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly; the NAT function can be disabled.

Obtain DNS Automatically: Select this checkbox to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

NOTE: If you are not familiar with these settings, please consult with ISP for further assistance or information.



After inserting your 3G/4G SIM card, please wait for 30 seconds before the dial-up connection process. If errors occur, please remove your SIM card or restarting your BEC 6200WZL router.

WAN Profile / Mobile Usage Allowance – Detailed setup instruction

Usage Allowance ☐ Enable

Configuration

Mobile Usage Allowance

Parameters

Mode

☐ Volume-based
☐ Time-based

MB data volume per month included
 hours per month included
 The billing period always begins on day of a month.

Over usage allowance action

E-mail Alert

Save the statistics to ROM

Disable

Apply

In order to query online time or volume used, you can set the following options.

Mode: Two methods are provided, that is, **Volume-based** and **Time-based**.

- ▶ **Volume-based:** If choosing **Volume-based**, you can view the volume you have used.
- ▶ **Time-based:** If choosing **Time-based**, you can view the online hours you have used.

Volume-based

Parameters

Mode

☒ Volume-based
☐ Time-based

MB data volume per month included
 hours per month included
 The billing period always begins on day of a month.

Over usage allowance action

E-mail Alert

Save the statistics to ROM

Disable

Apply

Only Download: Only make statistics of Download Traffic.

Only Upload: Only make statistics of Upload Traffic.

Download and Upload: Make statistics of both Download and Upload Traffic.

Time-based

Allow you to manually assign a billing period.

Parameters	
Mode	<input type="radio"/> Volume-based Only Download <input type="text"/> MB data volume per month included
	<input checked="" type="radio"/> Time-based 720 <input type="text"/> hours per month included The billing period always begins on day 1 <input type="text"/> of a month.
Over usage allowance action	E-mail Alert <input type="button" value="v"/>
Save the statistics to ROM	Disable <input type="button" value="v"/>

Over usage allowance action: If the online time or traffic you have used exceeds the usage allowance you set. The system will do the followings operations.

E-mail Alert and Disconnect <input type="button" value="v"/>
E-mail Alert
E-mail Alert and Disconnect
Disconnect

Save the statistics to ROM: Choose the time interval for saving statistics. You can choose to save for **Every one hour** or **Disable** the function.

Every one hour <input type="button" value="v"/>
Every one hour
Disable

System

The **System** section contains instruction for setting up local time zone, updating device system firmware, retrieving current device configuration for a copy or restoring a saved configuration file when accidentally misconfigured the device, managing your login device information or setting up multiple account levels for others to access to this router, and send mail alert to inform you changes of your settings.

Time Zone

Configuration

Time Zone

Parameters

Time Zone

☒ Enable ☐ Disable

Local Time Zone (+-GMT Time)

(GMT-06:00) Central Time (US & Canada)

SNTP Server

192.43.244.18

128.138.140.44

129.6.15.29

131.107.1.10


Daylight Saving

☒ Automatic

Resync Period

1440

minutes



Apply

Cancel

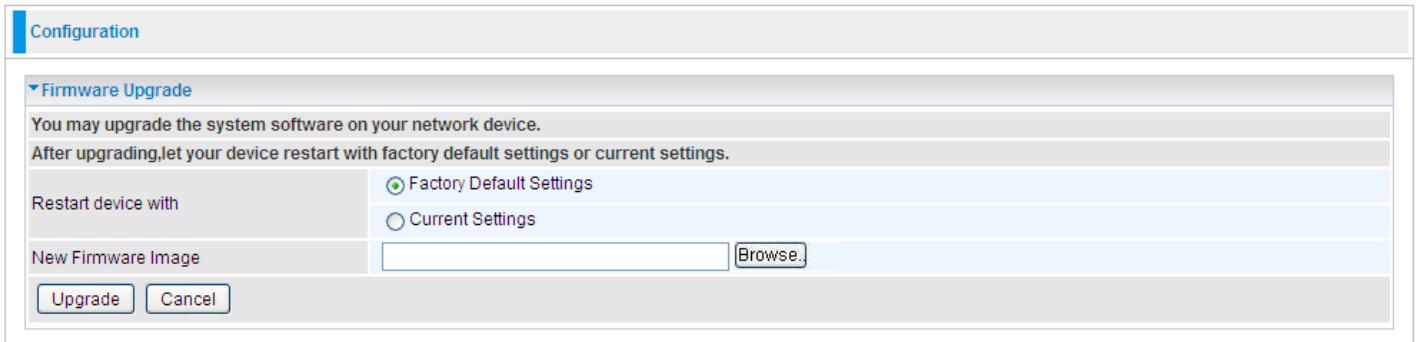
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router retrieves the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Resync Period (in minutes) is the periodic interval the router waits before it resynchronizes the router's time with that of the specified SNTP server. To avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

Firmware Upgrade

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified. Your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** allows you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.



Restart Device with: To choose "Factory Default Settings" or "Current Settings" which uses your current setting on the new firmware (it is highly advised to use Factory Default Settings over Current Settings for a clean firmware upgrade).

New Firmware Image: Type in the location of the file you wish to upload in this field or click **Browse...** to locate it.

Browse...: Click **Browse...** to find the file with the **.afw** file extension that you wish to upload.

NOTE: You must uncompress / unzip the **.zip** file before you can upgrade the file.

Upgrade: Click **upgrade** to begin the upload process. This process may take up to three minutes.



Warning

Do not power down the router or interrupt the firmware upgrade while it is still in process. Improper operation may damage the router. If firmware upgrade failure occurs, please refer to operations below for emergency recovery.

Recovery Procedure

If your device's upgrade failed, then you can take emergency recovery procedure to recover. Usually, if the device failed to upgrade successfully, the recovery page will automatically (or you enter 192.168.1.254 at the address bar) turn to the page showed as below, entering the recovery mode.

Recovery Code

Bootrom Version: 1.09

- ☒ Reset to factory default settings
☐ Keep current settings

Enter the path and name of the upgrade file then click the START button below. You will be prompted to confirm the upgrade. The device will be successfully upgraded when the System LED stops blinking.

Browse..

START

Select the correct file used for upgrade, and press **START**.

Backup / Restore

It allows you to save and backup your router's current settings, in a readable format, on your PC, or to restore a previously saved configuration. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. Highly recommended you backup your router's settings before and after any changes to your router.

The screenshot shows a web interface with a 'Configuration' tab selected. Under the 'Backup/Restore' section, there is a description: 'Allows you to backup the configuration settings to your computer, or restore configuration from your computer.' Below this, the 'Backup Configuration' section has the text 'Backup configuration to your computer.' and a 'Backup' button. The 'Restore Configuration' section has a 'Configuration File' input field, a 'Browse...' button, and a 'Restore' button. A warning message states: 'Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.'

Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse...** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

Select the settings files you wish to use, and press **Restore** to load those settings into the router.

Restart Router

Click **Restart** with option **Current Settings** to reboot your router and save the current configuration to device.

The screenshot shows a web interface with a 'Configuration' tab selected. Under the 'Restart' section, there is a description: 'After restarting. Please wait for several seconds to let the system come up.' Below this, the 'Restart device with' section has two radio button options: 'Factory Default Settings' and 'Current Settings'. The 'Current Settings' option is selected. A 'Restart' button is located at the bottom of the section.

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

User Management

Configuration

▼ User Priority Setup

Parameters

High Priority User

Guest

Apply

Cancel

▼ User Management

Parameters

Valid	User	Password	Confirm	Login Mode	Level
<input type="checkbox"/>				Basic	Super

Add

Edit / Delete

Edit	Valid	User	Login Mode	Level	Delete
<input type="radio"/>	true	admin	Basic	Super	Administrator

In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Add** new users who are able to access the device's configuration interface. Once you have clicked **Edit** on the account you want to edit, the information of the account will be displayed above. Just go ahead and change the password.

You can change the user's **password**, whether their account is active and **Valid**. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking ticking the box under **Delete** and then press the **Edit/Delete** button.

It is highly recommended to change your router password to something unique that only you know it when you receive this unit. If at any time you forget this password, please press and hold the RESET button in the rear panel for more than 6 seconds then release it for router to restore to its factory default settings.

Mail Alert

Mail Alert is designed to keep you as the router administrator or other relevant personnel alerted of any change to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.

Configuration		
▼ Mail Alert		
Server Information		
SMTP Server	<input type="text"/>	
Username	<input type="text"/>	
Password	<input type="text"/>	
Sender's E-mail	<input type="text"/>	(Must be xxx@yyy.zzz)
Failover / Failback		
Recipient's E-mail	<input type="text"/>	(Must be xxx@yyy.zzz)
WAN IP Change Alert		
Recipient's E-mail	<input type="text"/>	(Must be xxx@yyy.zzz)
Mobile Overran Allowance		
Recipient's E-mail	<input type="text"/>	(Must be xxx@yyy.zzz)
Intrusion Detection		
Alert Mail Time	<input type="text" value="30"/>	min(s)
Recipient's E-mail	<input type="text"/>	(Must be xxx@yyy.zzz)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

Recipient's Email (Failover / Failback): Enter the email address that will receive the alert message once a computer / network server failover occurs.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert message once a WAN IP change has been detected.

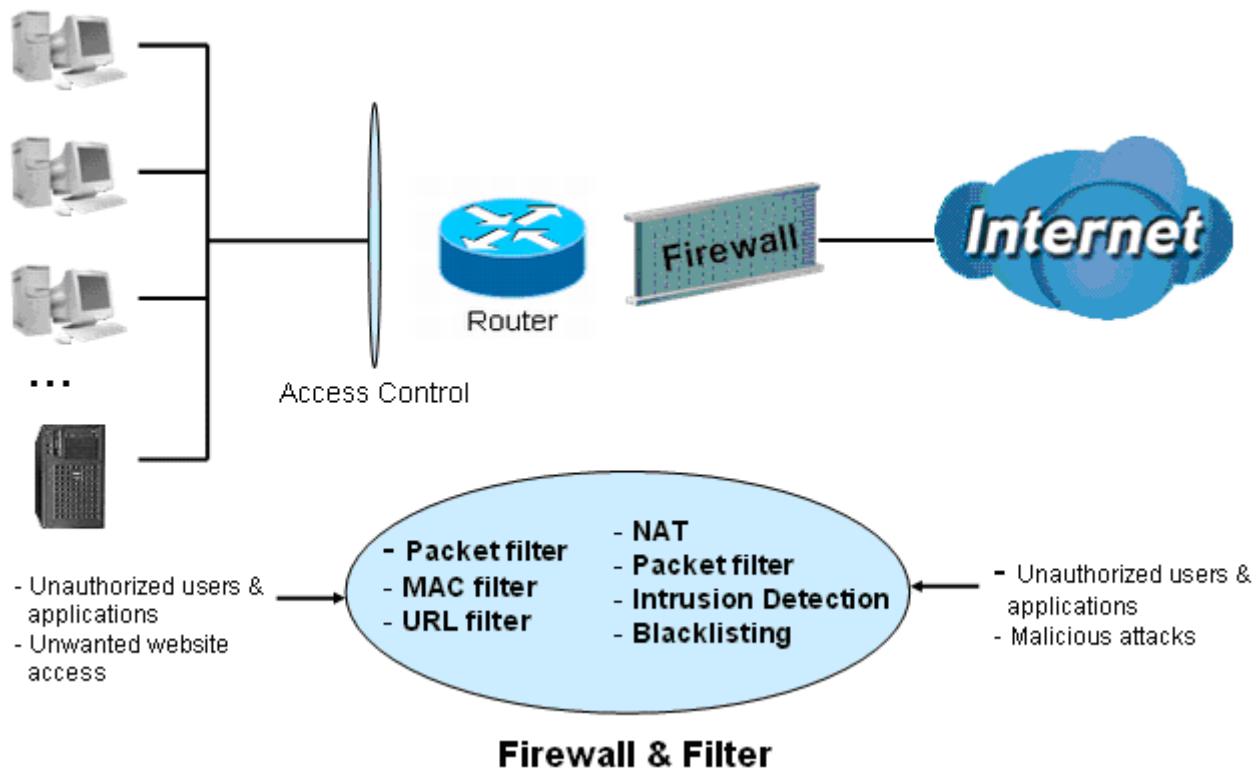
Recipient's Email (Mobile Overran Allowance): Enter the email address that will receive the alert message once 3G / 4G overran allowance was detected.

Alert Mail Time (Intrusion Detection): The time interval of sending Email.

Recipient's Email (Intrusion Detection): Enter the email address that will receive the alert message once intrusion has been detected.

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the **WAN** configuration section for more details on NAT.



Firewall: Prevents access from outside your network.

NAT natural firewall: This masks LAN users' IP addresses, which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when the NAT function is enabled.



When using Virtual Servers (port mapping) your PCs are exposed to the ports specified opened in your firewall packet filter settings.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent, and log malicious attacks.

MAC Filter rules: Prevents unauthorized computers accessing the Internet.

URL Filter: Blocks PCs on your local network from unwanted websites.

Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. This configuration program allows you to set up to 6 different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is “**or**” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Edit	Order	Rule Name	Internal IP Address	External IP Address	Protocol	Internal Port	External Port	Direction	Action	Time Schedule	Delete
		Default	Any	Any	Any	Any	Any	outgoing	forward	Always On	

Rule Name: Users-define description to identify this entry. The maximum name length is 32 characters, and then can choose application that they want from list box.

Internal IP Address / External IP Address: This is the Address-Filter used to allow or block traffic to/from particular IP addresses. Input the range you want to filter out. If you leave empty or 0.0.0.0, it means any IP address.

Protocol: Specify the packet type (TCP, UDP, ICMP, etc.) that the rule applies to.

Select **TCP** if you wish to search for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to search for the connectionless application service on the remote server using the port number.

Action: If a packet matches this filter rule, **Forward (allows the packets to pass)** or **Drop (disallow the packets to pass)** this packet.

Internal Port: This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535**. It is recommended that this option be configured by an advanced user.

External Port: This is the Port or Port Range that defines the application.

Direction: Determine whether the rule is for outgoing packets or for incoming packets.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.

Log: Choose “log” if you wish to generate logs when the filter rule is applied to a packet.

Add: Click this button to add a new packet filter rule and the added rule will appear at the bottom table.

Edit: Check the Rule No. you wish to edit, and then click “Edit”.

Delete: Check the Rule No. you wish to delete, and then click “Delete”.

Edit	Order	Rule Name	Internal IP Address	Protocol	Internal Port	Direction	Action	Time Schedule	Delete
			External IP Address		External Port				
<input type="radio"/>	↓	FTP	Any	TCP	Any	outgoing	forward	Always On	<input type="checkbox"/>
			Any		21~21				
<input type="radio"/>	↑	TELNET	Any	TCP	Any	outgoing	forward	Always On	<input type="checkbox"/>
			Any		23~23				
		Default	Any	Any	Any	outgoing	forward	Always On	
			Any		Any				



Attention

If the DHCP server option is enabled, you must be very careful in assigning IP addresses of a filtered private IP range to avoid conflicts because you do not know which PC in the LAN is assigned which IP address. The easiest and safest way is that the filtered IP address is assigned to a specific PC that is not allowed to access an outside resource such as the Internet. You configure the filtered IP address manually for this PC, but it stays in the same subnet with the router.

MAC Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules; you can add the filter rules to meet your requirements.

The screenshot shows a web-based configuration interface for a MAC Filter. At the top, there is a 'Configuration' tab. Below it, the 'MAC Filter' section is expanded. Under 'Filter Action', there are three radio buttons: 'Disable', 'Allow', and 'Block'. The 'Block' option is selected. An 'Apply' button is located below the radio buttons. Under the 'Parameters' section, there is a 'MAC Address' field with a text input and a dropdown menu showing '<< --select--'. To the right of the dropdown is a note '(type or select from listbox)'. Below the 'MAC Address' field is a 'Time Schedule' dropdown menu showing 'Always On'. At the bottom of the 'Parameters' section, there are two buttons: 'Add' and 'Edit / Delete'.

Action: select to determine how to do with the filter.

- ▶ **Disable:** to disable the MAC filter function.
- ▶ **Allow:** to enable the MAC filter function and allow the host of the following set MAC addresses to access.
- ▶ **Block:** to enable the MAC filter function and block the host of the following set MAC addresses to access.

MAC Address: Enter the MAC addresses you wish to manage.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.

Intrusion Detection

Check Enable if you wish to detect intruders accessing your computer without permission. The router automatically detects and blocks a DoS (Denial of Service) attack if a user enables this function. This kind of attack is not to access confidential data on the network; instead, it aims to disrupt specific equipment or the entire network. If this happens, users will have trouble accessing the network resources.

The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'Intrusion Detection' section is expanded. Under the 'Parameters' heading, there are four rows of configuration options:

Parameters	
Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Maximum TCP Open Handshaking Count	<input type="text" value="100"/> per second
Maximum Ping Count	<input type="text" value="15"/> per second
Maximum ICMP Count	<input type="text" value="100"/> per second
Log	<input type="checkbox"/>

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

Intrusion Detection: Check Enable if you wish to detect intruders accessing your computer without permission.

Maximum TCP Open Handshaking Count: This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Maximum Ping Count: This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Maximum ICMP Count: This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

Log: Check Log if you wish to generate logs when the filter rule is applied to the Intrusion Detection.

For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log but it will not be able to protect against such attacks.

Hacker attack types recognized by the IDS

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP

Src Port: Source Port

Dst Port: Destination Port

Dst IP: Destination IP

Block WAN PING

Check Enable if you wish to exclude outside PING requests from reaching this router.

The screenshot shows the 'Configuration' tab with the 'Block WAN PING' section expanded. Under 'Parameters', the 'Block WAN PING' option is set to 'Disable' (indicated by a green dot). There are 'Apply' and 'Cancel' buttons at the bottom.

URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of <http://www.example.com>) filter rules allow you to prevent users on your network from accessing particular websites from their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.

The screenshot shows the 'Configuration' tab with the 'URL Filter' section expanded. Under 'Parameters', the following settings are visible: 'Keywords Filtering' (unchecked), 'Domains Filtering' (unchecked), 'Restrict URL Features' (Block: unchecked for Java Applet, ActiveX, Cookie, and Proxy), 'Except IP Address' (Detail link), 'Time Schedule' (Always On dropdown), and 'Log' (unchecked). There are 'Apply' and 'Cancel' buttons at the bottom.

Keywords Filtering

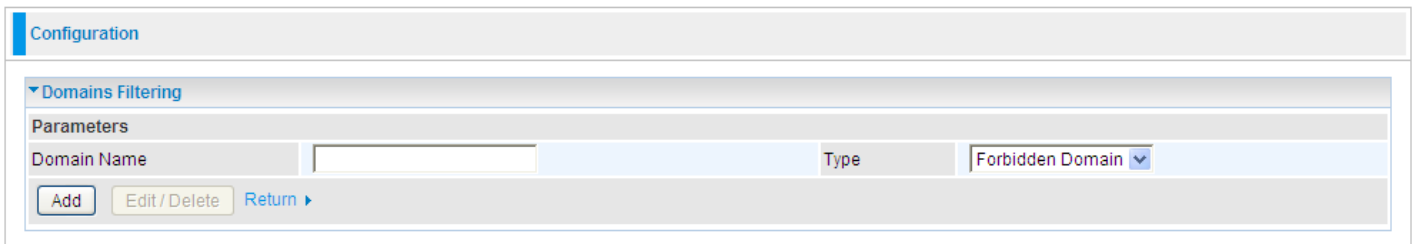
Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list is checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, the URL <http://www.abc.com/abcde.html> would be dropped since the keyword “abcde” occurs in the URL.

The screenshot shows the 'Configuration' tab with the 'Keywords Filtering' section expanded. Under 'Parameters', there is a 'Keyword' text input field. Below it are 'Add', 'Edit / Delete', and 'Return' buttons.

Domain Filtering

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, it is checked with the forbidden list. If present, the connection attempt is dropped.
3. If the packet matches neither of the above, it is sent to the remote web server.
4. Please be note that the completed URL, “www” + domain name shall be specified. For example to block traffic to www.google.com.au, enter “www.google” or “www.google.com”



Restrict URL Features

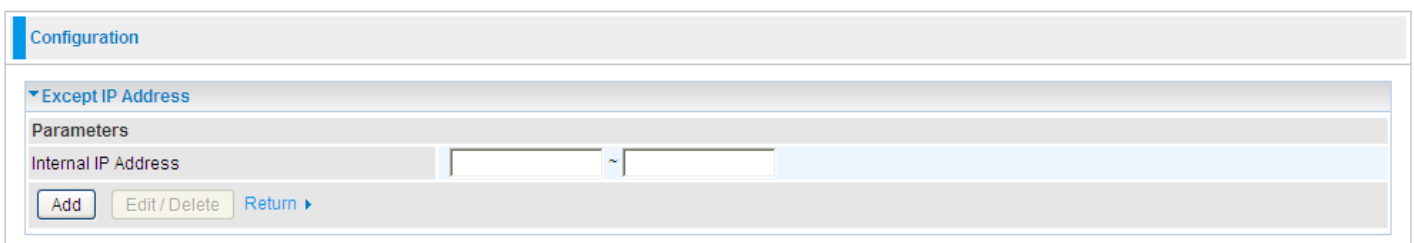
The router will automatically filter out the selected features.

- ▶ **Block Java Applet:** Blocks Java Applet
- ▶ **Block ActiveX:** Blocks ActiveX
- ▶ **Block Cookies:** Blocks Cookies
- ▶ **Block Proxy:** Blocks Proxy

Except IP Address

Once enabled, the URL filtering will apply to all devices that are associating with the router.

If you wish to be excluded from the filtering group, please enter your device’s IP or an IP range.



Time Schedule

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log

Log: Click “Log” if you wish to generate logs when the filer rule is applied to the URL Filter.

QoS - Quality of Service

Quality of Service Introduction

If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in the routers is such a breakthrough for home users and office users.

QoS: Keeping Your Net Connection Fast and Responsive

Configurable by internal IP address, external IP address, protocol, and port, the Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring bandwidth-consumption data like gaming packets, latency-sensitive application like voice, or even mission critical files, move through the router at lightning speed, even under heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

QoS Setup

Please choose the **QoS** in the **Configuration** item of the left window as depicted below.

Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

Parameters

Application	<input type="text"/>	Direction	LAN to WAN
Protocol	Any	DSCP Marking	Disable
Rate Type	Guaranteed (Minimum)	Ratio	%
Internal IP Address	<input type="text"/> ~ <input type="text"/>	Internal Port	<input type="text"/> ~ <input type="text"/>
External IP Address	<input type="text"/> ~ <input type="text"/>	External Port	<input type="text"/> ~ <input type="text"/>
Time Schedule	Always On	Priority	Normal

After clicking the QoS item, you can Add/Edit/Delete a QoS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

Application: A name that identifies an existing policy.

Direction: The traffic flow direction to be controlled by the QoS policy.

There are two settings to be provided in the Router:

- ▶ **LAN to WAN:** You want to control the traffic flow from the local network to the outside world. e.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QoS policy. So, you need to add a policy with LAN to WAN direction setting.
- ▶ **WAN to LAN:** Control Traffic flow from the WAN to LAN. The connection maybe either issued from LAN to WAN or WAN to LAN.)

Protocol: The Protocol will be controlled. For GRE protocol, there is no need to specify the IP

addresses or Application ports in this page. For other protocols, at least one value shall be given.

- **ANY:** No protocol type is specified.
- **TCP**
- **UDP**
- **ICMP**
- **GRE**

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify traffic based on DSCP value and send packets to next Router.

NOTE: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

The DSCP Mapping Table

DSCP Mapping Table	
3G / 4G Router	Standard DSCP
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Rate Type: 2 types are provided:

- ▶ **Limited (Maximum):** Specify a limited data rate for this policy. It also is the maximal rate for this policy. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.
- ▶ **Guaranteed (Minimum):** Specify a minimal data rate for this policy. For example, you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidth. You can use this type. Then, if there is available bandwidth that is not used, it will be given to this policy by following priority assignment.

Ratio: Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20.

Priority: Specify the priority for the bandwidth that is not used. For examples, you may specify two different QoS policies for different applications. Both applications need a minimal bandwidth and need more bandwidth, beside the assigned one, if there is any available/non-used one available. So, you may specify which application can have higher priority to acquire the non-used bandwidth.

- ▶ **High**
- ▶ **Normal:** The default is normal priority.
- ▶ **Low**

For the sample priority assignment for different policies, it is served in a First-In-First-Out way.

Internal IP Address: The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

Internal Port: The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

External IP Address: The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

External Ports: The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

Time Schedule: Scheduling your prioritization policy.

Example: QoS for your Network

If you are actively engaged in using P2P and are afraid of slowing down internet access throughput of other users within your network, you can thus use QoS function to set different priorities and bandwidth ratio for the different applications that members of your network will be using to avoid bandwidth traffic from getting overloaded.

The figures below are a simple example to show the different settings for Web Browsing and Email sending to assure the bandwidth for these applications.

For Web Browsing (HTTP)

Here we guarantee 50% of the traffic for HTTP application.

Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

Parameters

Application	HTTP	Direction	LAN to WAN		
Protocol	TCP	DSCP Marking	Gold service(L)		
Rate Type	Guaranteed (Minimum)	Ratio	50 %	Priority	High
Internal IP Address			Internal Port		
External IP Address			External Port		
Time Schedule	Always On				

Add

Edit / Delete

For Mail Sending (SMTP)

Here we guarantee 30% of the traffic for Mail application.

Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 50% Downstream (WAN to LAN) : 100%

Parameters

ApplicationSMTP
DirectionLAN to WAN

ProtocolTCP
DSCP MarkingGold service(M)

Rate TypeGuaranteed (Minimum)
Ratio30 %
PriorityHigh

Internal IP Address
Internal Port

External IP Address
External Port

Time ScheduleAlways On

Add
Edit / Delete

Edit	Application	Direction	Rate Type	Ratio	Time Schedule	Delete
<input type="radio"/>	HTTP	LAN to WAN	Guaranteed	50%	Always On	<input type="checkbox"/>

Edit	Application	Direction	Rate Type	Ratio	Time Schedule	Delete
<input type="radio"/>	HTTP	LAN to WAN	Guaranteed	50%	Always On	<input type="checkbox"/>
<input type="radio"/>	SMTP	LAN to WAN	Guaranteed	30%	Always On	<input type="checkbox"/>

thus, 20% of LAN to WAN (upstream) traffic is reserved for other uses and those applications' bandwidths are guaranteed.

For downstream traffic bandwidth, just the direction changes and the configuration are similar.

BEC 6200WZL User Manual

Virtual Server

In TCP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

The reason is that when using NAT, your publicly accessible IP address is used by and points to your router, which needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for information on NAT.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports”. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports, or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA's website at: <http://www.iana.org/assignments/port-numbers>

Well-known and Registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Port Mapping

The screenshot shows the 'Configuration' tab with the 'Port Mapping' section expanded. The 'Parameters' section includes fields for 'Application' (a dropdown menu), 'Protocol' (a dropdown menu with 'TCP' selected), 'External Port' (a range input), 'Internal IP Address' (a dropdown menu), 'Internal Port' (a range input), and 'Time Schedule' (a dropdown menu with 'Always On' selected). At the bottom of the form are two buttons: 'Add' and 'Edit / Delete'.

Application: Select the service you wish to configure.

Protocol: Automatic when you choose Application from list-box or select a protocol type which you want.

External Port & Internal Port: Enter the public port number & range you wish to configure.

Internal IP Address: Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

Add: Click to add a new virtual server rule. Click again and the next figure appears.

Edit: Check the Rule No. you wish to edit and then click “Edit/Delete”.

Delete: Check the Rule No. you wish to delete then click “Edit/Delete”.

Since NAT acts as a “natural” Internet firewall, your router protects your network from access by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request to the router for a specified port is received, it is forwarded to the corresponding internal server.

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

The screenshot shows the 'Configuration' tab with the 'Port Mapping' section expanded. The 'Parameters' section is the same as in the previous screenshot. Below the form is a table of existing rules. The 'Add' button is highlighted with a red circle, and the 'Edit / Delete' button is highlighted with a red rectangle. The table has columns for 'Edit', 'Application', 'Protocol', 'External Port', 'Internal IP Address', 'Internal Port', 'Time Schedule', and 'Delete'.

Edit	Application	Protocol	External Port	Internal IP Address	Internal Port	Time Schedule	Delete
<input type="radio"/>	FTP	TCP	21~21	192.168.1.100	Any	Always On	<input type="checkbox"/>
<input checked="" type="radio"/>	HTTP	TCP	80~80	192.168.1.10	Any	Always On	<input type="checkbox"/>

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by the particular application. Most applications use TCP or UDP; however you

can specify other protocols using the drop-down **Protocol** menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets are checked by the Firewall and NAT algorithms, it is then passed to the DMZ host when a packet received does not use a port number in use by any other Virtual Server entries.

Configuration

DMZ

Parameters

Internal IP Address: << --select-- (type or select from listbox)

Time Schedule: Always On

Except Ports

Port: << --select--

Protocol: TCP

Description: **Add**

Except List

ID	Description	Protocol	Port	Operation
----	-------------	----------	------	-----------

Apply **Cancel**

Internal IP Address: Enter the IP address of a specific internal server to which will be the DMZ Host.

Time Schedule: A self defined time period. You may specify a time schedule. For setup and detail, refer to Time Schedule section.

Port: The except port number. Default is set from range 1 ~ 65535. You can select from the drop down list and also can enter manually.

Protocol: Select the TCP or UDP protocol from the drop down list.

Description: The description of the port's function.

Add/Delete Except Ports

1. Enter except port number in the port field or choose from the drop down list. Select the port and describe the port.

Except Ports

Port: 80 << Remote Access (TCP 80)

Protocol: TCP

Description: Remote Access **Add**

2. Click **Add**. The new except port will display below.

Except List				
ID	Description	Protocol	Port	Operation
1	Remote Access	tcp	80	Delete

3. Click **Delete** to delete the one which you want to remove from the except list.

Except List				
ID	Description	Protocol	Port	Operation
1	Remote Access	tcp	80	Delete
2	Printer Server	tcp	631	Delete
3	Web Cam	tcp	8081	Delete



Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.

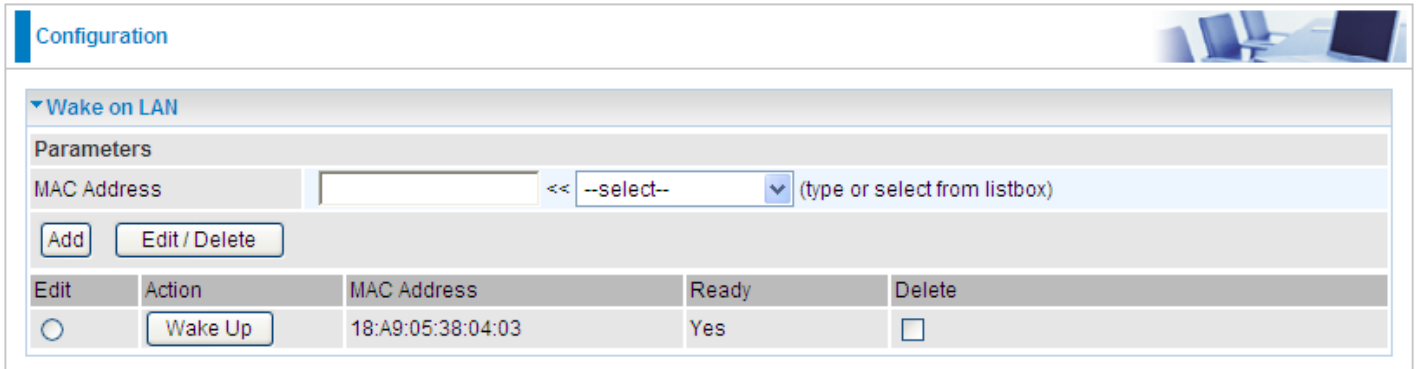


Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is disabled, you have to be very careful in assigning the IP addresses of the valid servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP addresses to each virtual server PC with an address that does not fall into the range of IP address that are issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Wake on LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.



Edit	Action	MAC Address	Ready	Delete
<input type="radio"/>	Wake Up	18:A9:05:38:04:03	Yes	<input type="checkbox"/>

Select: Select MAC address of the computer that you want to wake up or turn on remotely.

Add: After selecting, click **Add** then you can perform the Wake-up action.

Edit/Delete: Click to edit or delete the selected MAC address.

Ready:

- ▶ "Yes" indicating the remote computer is ready for your waking up.
- ▶ "No" indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.

Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. Your router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.

Configuration

Time Schedule

Parameters

Name
Day in a week

☐ Sun
☐ Mon
☐ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat

Start Time

08 : 00

End Time

18 : 00

Edit / Clear

Edit	Name	Day in a week	Start Time	End Time	Clear
<input type="radio"/>	TimeSlot1	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot2	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot3	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot4	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot5	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot6	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot7	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot8	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot9	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot10	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot11	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot12	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot13	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot14	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot15	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot16	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	08:00	18:00	<input type="checkbox"/>

Name: A user-defined description to identify this time portfolio.

Day in a week: The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.

Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule. Select the Apply button to apply your changes.

Advanced

Configuration options within the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Static Route

The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, a section titled 'Static Route' is expanded. Under this section, there is a 'Parameters' table with five columns: 'Destination', 'Netmask', 'Gateway', 'Interface', and 'Cost'. Each column has a corresponding input field. The 'Interface' field has a dropdown arrow. Below the table, there are two buttons: 'Add' and 'Edit / Delete'.

Destination	Netmask	Gateway	Interface	Cost
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>

Destination: The destination subnet IP address.

Netmask: Subnet mask of the destination IP addresses based on above destination.

Gateway: The gateway IP address to which packets are forwarded.

Interface: Select the interface through which packets are forwarded.

Cost: Represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

Static ARP

The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, a section titled 'Static ARP' is expanded. Under this section, there is a 'Parameters' table with two columns: 'IP Address' and 'MAC Address'. Each column has a corresponding input field. Below the table, there are two buttons: 'Add' and 'Edit / Delete'.

IP Address	MAC Address
<input type="text"/>	<input type="text"/>

IP Address: Fill in the IP address of the host computer that is sending the data packet.

MAC Address: Fill in the MAC address of the computer that the incoming data packets are to be forwarded.

Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful for hosting servers via your 3G / 4G connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>.

The screenshot shows a web interface for configuring Dynamic DNS. At the top, there is a 'Configuration' tab. Below it, the 'Dynamic DNS' section is expanded. Under 'Parameters', there are several fields: 'Dynamic DNS' with radio buttons for 'Enable' and 'Disable' (currently 'Disable' is selected); 'Dynamic DNS Server' with a dropdown menu showing 'www.dyndns.org (dynamic)'; 'Wildcard' with a checkbox labeled 'Enable' (currently unchecked); 'Domain Name', 'Username', and 'Password' each with a text input field; and 'Period' with a numeric input field set to '28' and a dropdown menu set to 'Day(s)'. At the bottom of the configuration area are 'Apply' and 'Cancel' buttons.

Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The fields following are activated and required.

Dynamic DNS Server: Select the DDNS service you have established an account with.

Wildcard: Select this check box to enable the DYNDNS Wildcard.

Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.

The screenshot shows a web interface for configuring a router. At the top, there is a 'Configuration' tab. Below it, the 'Device Management' section is expanded. It contains several settings: 'Device Host Name' with a sub-field 'Host Name' set to 'home.gateway'; 'Embedded Web Server' with 'HTTP Port' set to '80' (with a note '(The default HTTP port number is 80.)') and 'Expire to auto-logout' set to '3 min(s)'; and 'Universal Plug and Play (UPnP)' with 'UPnP' set to 'Enable' (radio button selected) and 'UPnP Port' set to '2800'. At the bottom of the section are 'Apply' and 'Cancel' buttons.

Embedded Web Server

HTTP Port: The port number of the router's embedded web server (for web-based configuration uses). The default value is the standard HTTP port, 80. You may specify an alternative if, for example, you are running a web server on a PC within your LAN.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.1.55**, and sets the logout time to be **100** minutes. The router only allows User A access from the IP address **192.168.1.55** to logon to the Web GUI by typing: <http://192.168.1.254:100> in their web browser. After 100 minutes, the device automatically logs out User A.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Disable: Check to disable the router's UPnP functionality.

Enable: Check to enable the router's UPnP functionality.

UPnP Port: The Default setting is 2800. It is highly recommended you use this port value.

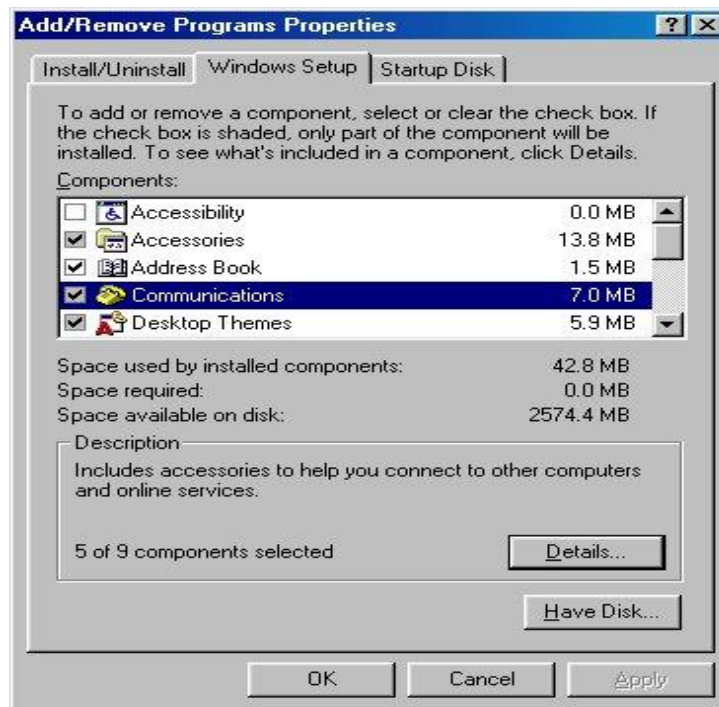
If this value conflicts with other ports already in use you may wish to change the port.

Installing UPnP in Windows Example

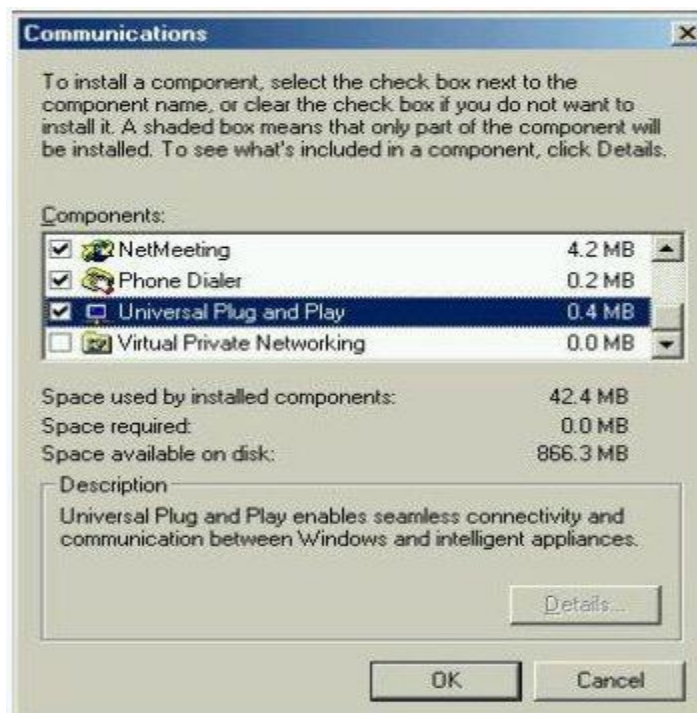
Follow the steps below to install the UPnP in Windows ME.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

Step 5: Restart the computer when prompted.

Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

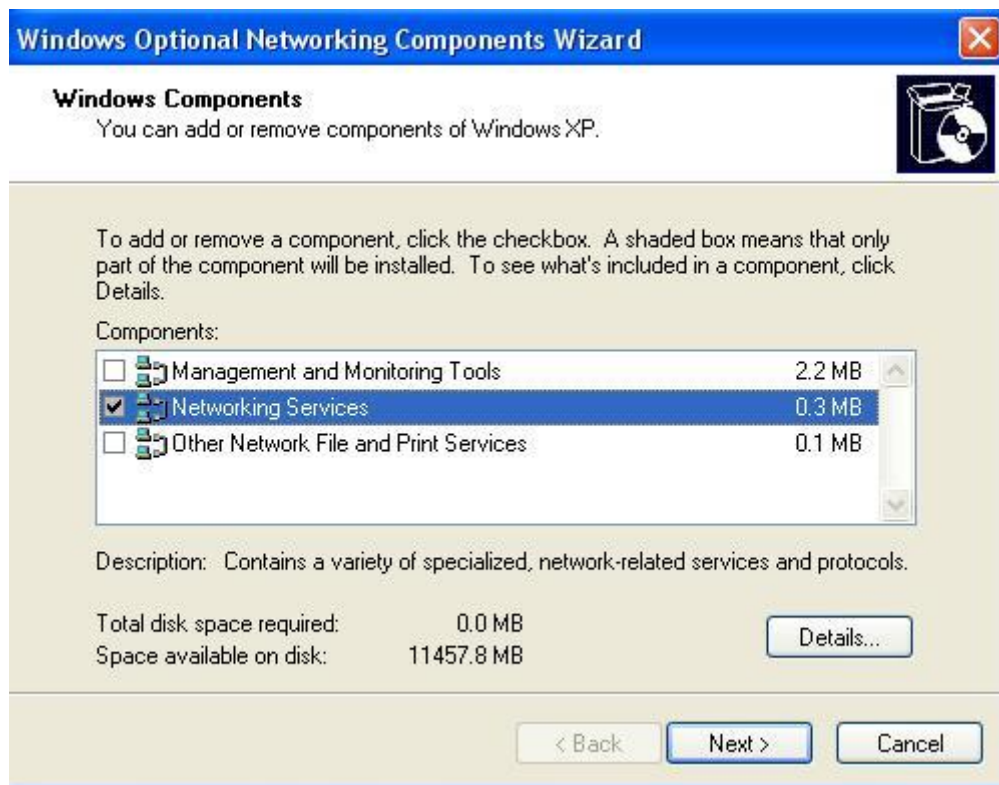
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components



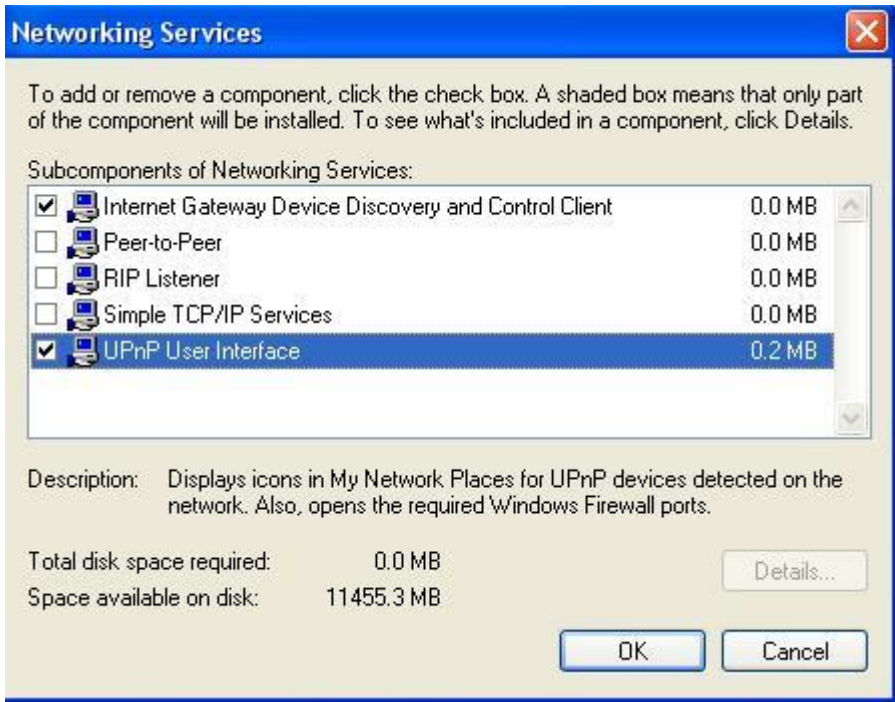
The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.



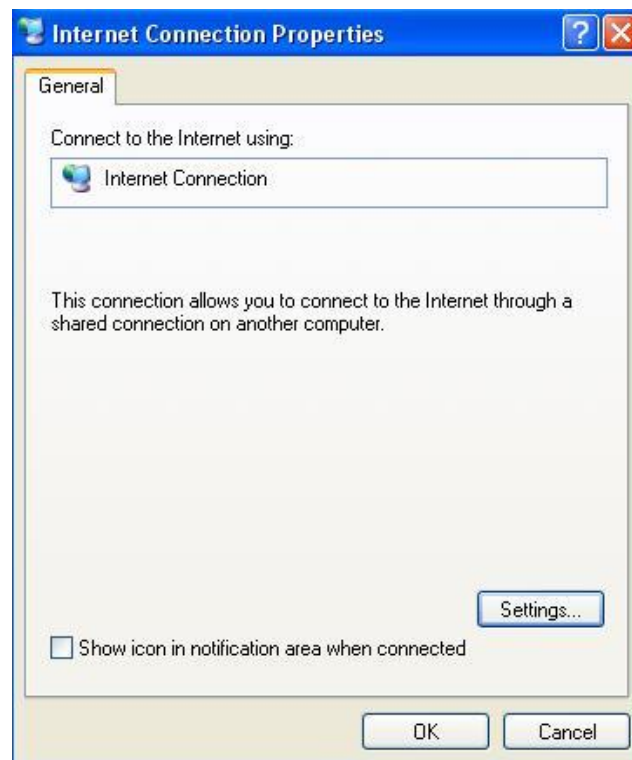
Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

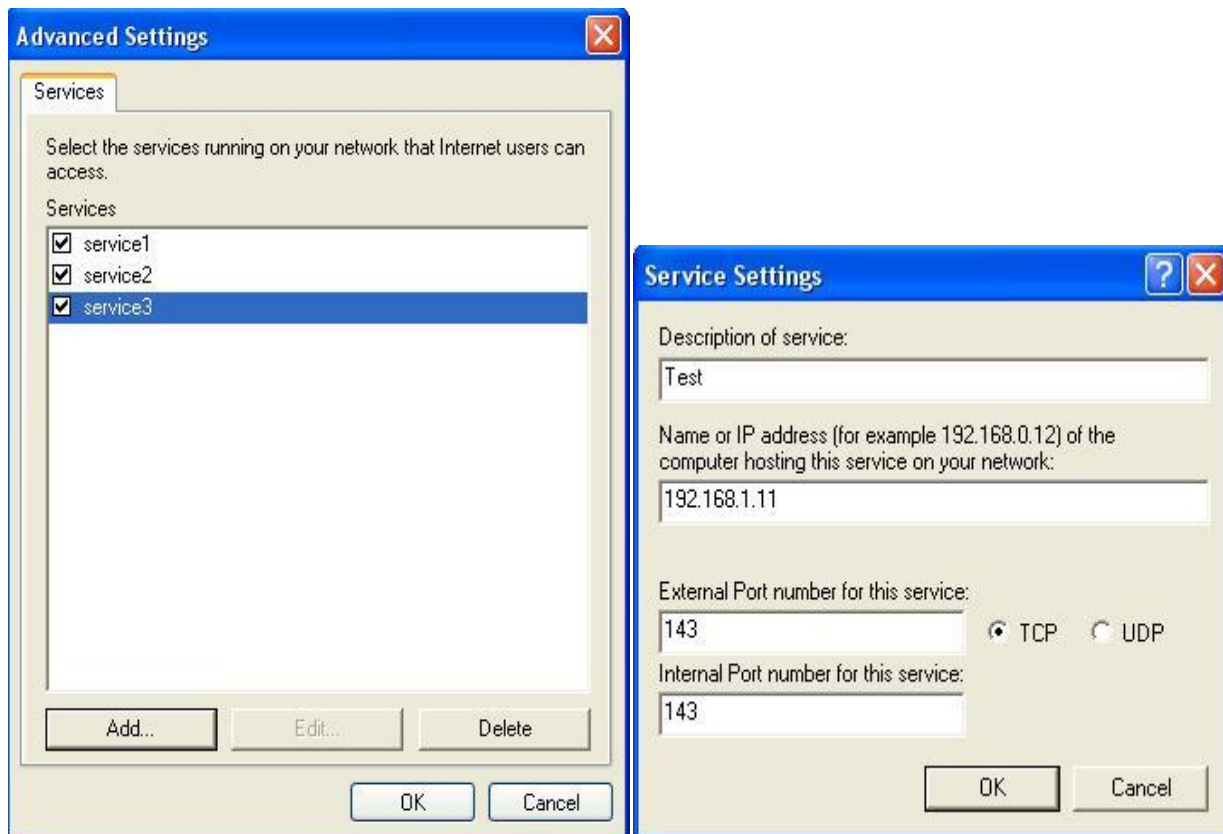
Step 2: Right-click the icon and select Properties.



Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray



Step 6: Double-click on the icon to display your current Internet connection status.



Easy Management and Access to the Router

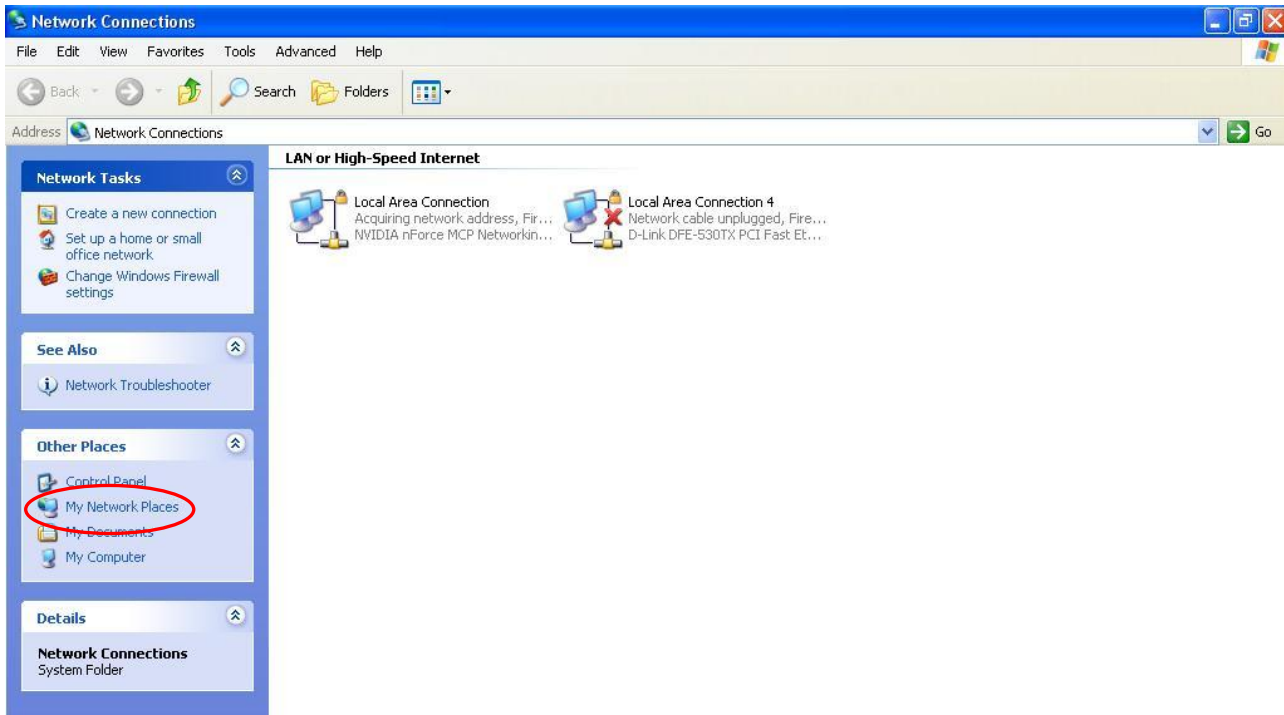
With UPnP, you can access web-based configuration for the **BEC 6200WZL** without first finding out the IP address of the router. This helps if you do not know the router's IP address.

Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your **BEC 6200WZL** and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your **BEC 6200WZL** and select Properties. A properties window displays basic information about the router.

SIP_ALG

Select **Enable** to activate **SIP ALG** feature or Disabled to disable this feature.

The Session Initiation Protocol (SIP) is an IETF-defined signaling protocol, widely used for controlling multimedia communication sessions such voice and video calls over Internet protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. It is a text-based Application Layer protocol.

But as many use NAT to communicate with the public networks, and the IP address and port combination in SIP packets are needed for addressing, we must come up with an effective way to deal with SIP NAT traversal. SIP ALG is an easy solution with which you are only required to enable SIP ALG on NAT application in this router to easily experience the smooth SIP connection between private networks and public networks or even in two private networks with your VoIP devices.

Parameters	
SIP_ALG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Apply Cancel

Port NAT

Port NAT is designed to separate LAN ports and Wireless interface to become, virtually, independent working groups that all share with the same WAN IP but different WAN interface.

Ethernet Port				WLAN Port				Interface
#1	#2	#3	#4	#1	#2	#3	#4	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	MOBILE_APN1
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	MOBILE_APN2
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	EWAN

Apply Cancel

For example,

A user has two 3G/4G APNs, and he can put Ethernet port1, port2 and wireless1(three ports mainly connected to devices for simple internet surfing) into a group, sharing interface MOBLE-APN1 to communicate with internet devices.

Separate Ethernet port3 and port4 (ports used to connect to audio and video devices or mainly access audio and video traffic) into another group sharing MOBLE_APN2.

Devices of each group work in an independent network without too much traffic loaded on one WAN interface, making each group relatively enjoy a pure internet environment.

Configuration

▼ Port NAT

Parameters

Ethernet Port				WLAN Port				Interface
#1	#2	#3	#4	#1	#2	#3	#4	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	MOBILE_APN1 ▼
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	MOBILE_APN2 ▼
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	EWAN ▼

Apply Cancel

IGMP

IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.

Configuration

▼ IGMP

Parameters

IGMP Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IGMP Snooping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply Cancel

IGMP Proxy: Accepting multicast packet. Default is set to **Disable**.

IGMP Snooping: Enable or disable the IGMP Snooping function. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group.”

SNMP Access Control

Software on a PC within the LAN is required in order to utilize this function - Simple Network Management Protocol.

The screenshot shows a web-based configuration interface for SNMP Access Control. At the top, there is a 'Configuration' tab. Below it, the 'SNMP Access Control' section is expanded. Under 'Parameters', there are radio buttons for 'Enable' and 'Disable', with 'Disable' selected. Below this, the 'SNMP V1 and V2' section contains two rows: 'Read Community' and 'Write Community'. Each row has a text input field for the community name and a text input field for the 'IP Address'. Below that, the 'SNMP V3' section contains a 'Username' text input field and a 'Password' text input field. At the bottom of the form are 'Apply' and 'Cancel' buttons.

SNMP V1 and V2

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

SNMP V3

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPV2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

- ☒ System group
- ☒ Interfaces group
- ☒ Address Translation group
- ☒ IP group
- ☒ ICMP group
- ☒ TCP group
- ☒ UDP group
- ☒ EGP (not applicable)
- ☒ Transmission
- ☒ SNMP group

From RFC1650 (EtherLike-MIB):

- ☒ dot3Stats

From RFC 1493 (Bridge MIB):

- ☒ dot1dBase group
- ☒ dot1dTp group
- ☒ dot1dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB):

- ☒ pppLink group
- ☒ pppLqr group

From RFC 1472 (PPP/Security MIB):

- ☒ PPP Security Group)

From RFC 1473 (PPP/IP MIB):

- ☒ PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

- ☒ PPP Bridge Group

From RFC1573 (IfMIB):

- ☒ ifMIBObjects Group

From RFC 1907 (SNMPv2):

only snmpSetSerialNo OID

TR-069 Client

TR069, (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones). At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.

The screenshot shows a web-based configuration interface for the TR-069 client. At the top, there is a tab labeled 'Configuration'. Below it, a section titled 'TR-069 client' is expanded, showing a 'Parameters' table. The table has two columns: a label column and a value column. The rows are: 'Inform' with radio buttons for 'Enable' and 'Disable' (where 'Disable' is selected); 'ACS URL' with a text input field; 'ACS Username' with a text input field; 'ACS Password' with a text input field; and 'Inform Period' with a text input field and a note '(0 means never send inform message to ACS)'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Parameters	
Inform	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
ACS URL	<input type="text"/>
ACS Username	<input type="text"/>
ACS Password	<input type="text"/>
Inform Period	<input type="text"/> (0 means never send inform message to ACS)

Apply Cancel

Inform: Enable to authorize CPE to send Inform message to automatically connect to ACS.

ACS URL: Enter the ACS server accessing URL.

ACS Username: Set the ACS user name for ACS authentication to the connection from CPE.

ACS Password: Set the ACS server login password.

Inform Period: Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS.

Remote Access

Configuration

▼ Remote Access

Parameters

Remote Access Control ☐ Enable Duration min(s) (0: Always On)

Apply

Allowed Access IP Address Range

Valid ☒ IP Address Range ~

Add Edit / Delete

Enable: Select Enable to allow management access from remote side (mostly from internet).

Duration: Set how many minutes to allow management access from remote side. Zero means always on.

Allowed Access IP Address Range

Valid: Select Valid to allow remote management from these IP ranges.

IP Address Range: Specify what IP address to be allowed to access device from remote side. Click Add to insert management IP address list.

Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click "**Save Config**" and click "**Apply**" to write your new configuration to FLASH.

Configuration

▼ Save Config to FLASH

Write settings to FLASH

Apply

Restart

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).

Configuration

▼ Restart

After restarting. Please wait for several seconds to let the system come up.

Restart device with

☐ Factory Default Settings
☒ Current Settings

Restart

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

Logout

To exit the router's web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes.

You can modify this value using the [Advanced / Device Management](#) section of the web interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

If your **BEC 6200WZL** is not functioning properly, you can refer to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or BEC for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problem with LAN Interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Recovery Procedures

Problem	Suggested Action
<ul style="list-style-type: none">- The front LEDs display incorrectly- Still cannot access to the router management interface after pressing the RESET button.- Software / Firmware upgrade failure	<ol style="list-style-type: none">1. Power on the router, once the Power LED lit red, please press this reset button using the end of paper clip or other small pointed object immediately.2. The router's emergency-reflash web interface will then be accessible via http://192.168.1.1 where you can upload a firmware image to restore the router to a functional state, Please note that the router will only respond with its web interface at this address (192.168.1.1), and will not respond to ping request from your PC or other telnet operations.

APPENDIX: PRODUCT SUPPORT & CONTACT

If you come across any problems please contact the dealer from where you have purchased the product.

Contact BEC @ <http://www.bectechnologies.net>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows ME, Windows XP, and Windows Vista are registered Trademarks of Microsoft Corporation.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ♦ Reorient or relocate the receiving antenna.
- ♦ Increase the separation between the equipment and receiver.
- ♦ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- ♦ Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.